(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11340966 A

(43) Date of publication of application: 10 . 12 . 99

(51) Int. Cl H04L 9/14
H04K 1/04
H04N 7/167

(21) Application number: 10145372

(22) Date of filing: 27 . 05 . 98

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

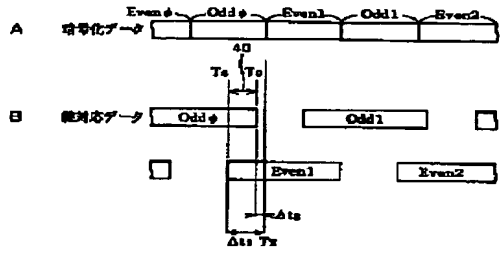
(72) Inventor: SUGIMOTO YOSHIYUKI

(54) SYSTEM AND METHOD FOR COMMUNICATION USING KEY

(57) Abstract:

PROBLEM TO BE SOLVED: To shorten the time for acquiring images or voices by shortening the time to be occupied for sending out a cryptographic key by sending out key correspondent data so as to correspond to not only a key at that time but also a key to be next used within a prescribed overlap period before the time of changing a key used in enciphered data.

SOLUTION: In the Fig. B, sections Odd0, Even1, Odd1 and Even2 are respectively periods for sending out the key correspondent data of cryptographic keys Odd0, Even1, Odd1 and Even2. Preceding to a time Tx to change the cryptographic key used in the enciphered data by Δt_1 (Ts), the next key correspondent data are sent out. This is for receiving data without interrupting them while considering the time for restoring the cryptographic key from the key correspondent data on the reception side. Besides, the key correspondent data of the cryptographic key just used or enciphering data at present as well are continuously sent out even after the transmission of the next key correspondent data is started. Thus, an overlap period 40 is provided.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－340966

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ	9/00	６４１
Ｈ０４Ｋ　1/04		Ｈ０４Ｋ	1/04	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ	7/167	Ｚ

審査請求　未請求　請求項の数19　ＯＬ　（全 30 頁）

(21)出願番号　特願平10－145372

(22)出願日　平成10年(1998)５月27日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　杉本　圭志
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

(74)代理人　弁理士　古谷　栄男　（外３名）

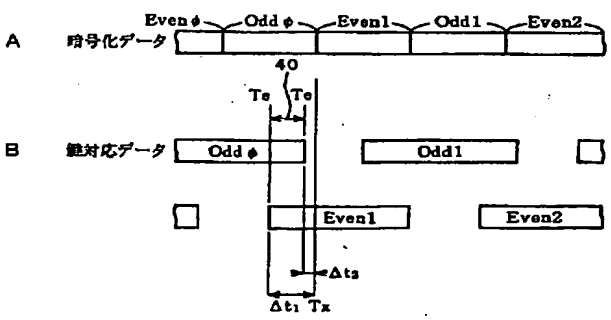
(54)【発明の名称】　鍵を用いた通信システムおよび方法

(57)【要約】

【課題】　暗号鍵送出のための占有時間が短く、かつ、受信開始時に、画像および音声が得られるまでの時間が短い通信システム、並びにかかるシステムにおいて所望の結果を得るための通信パラメータの設定を容易にすることを目的とする。

【解決手段】暗号化データと鍵対応データは、図２に示すようなタイミングにて送出される。図２Ｂに示すように、暗号化データにおいて用いた暗号鍵が変わる時点TxよりΔt_1だけ早く（Ts参照）、次の鍵対応データを送出している。これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、データが途切れることなく受信できるようにするためである。上記のように、一部において重複期間４０を設けることにより、鍵対応データによる通信路の占有をできるだけ小さくしつつ、特に処理開始時における受信側での復元データの連続的な受信を確保するようにしている。

暗号化データと鍵対応データの送出タイミング



【特許請求の範囲】
【請求項１】所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出する(a)送信装置と(b)受信装置とを備えた鍵を用いた通信システムであって：前記送信装置は、
(a1)順次異なる鍵を出力する鍵出力手段と、
(a2)鍵出力手段から取得した鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成する暗号化手段と、
(a3)鍵出力手段からの鍵を、対応する鍵対応データに変換する鍵対応データ生成手段と、
(a4)順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出する送出手段であって、暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出する送出手段と、
を備えており、
前記受信装置は、
(b1)送信されてくる暗号化データと鍵対応データとを受け取る受取手段と
(b2)受取手段によって受け取った鍵対応データに基づいて、鍵を生成する鍵取得手段と、
(b3)受取手段によって受け取った暗号化データを、鍵取得手段によって取得した鍵に基づいて復号化する復号化手段であって、暗号化データに対する処理の開始時点が前記重複期間外である場合は、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間である場合は、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始する復号化手段と、
を備えていることを特徴とする通信システム。
【請求項２】所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出し、受信側において暗号化データを復号化する通信方法であって、
順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、
順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、
暗号化データに用いた鍵が変わる時点より前の所定重複期間内において、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するとともに、
送出されてきた暗号化データと鍵対応データとを受け取り、
受け取った鍵対応データに基づいて鍵を生成し、
受け取った暗号化データを鍵に基づいて復号化するに際し、暗号化データに対する処理の開始時点が前記重複期間外である場合は、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間である場合は、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする通信方法。
【請求項３】所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出する送信装置であって、
順次異なる鍵を出力する鍵出力手段と、
鍵出力手段から取得した鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成する暗号化手段と、
鍵出力手段からの鍵を、対応する鍵対応データに変換する鍵対応データ生成手段と、
順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出する送出手段であって、暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出する送出手段と、
を備えた送信装置。
【請求項４】所定時間ごとに鍵を変えて送出すべきデータを暗号化して通信する通信方法であって、
順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、
順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、
暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出することを特徴とする通信方法。
【請求項５】請求項４の通信方法において、
前記重複期間においては、当該時点での鍵に対応する鍵対応データと、次に使用する鍵に対応する鍵対応データとの２つの鍵対応データを送出することを特徴とするもの。
【請求項６】請求項４の通信方法において、
前記重複期間においては、当該時点での鍵と次に使用する鍵とに対応する１つの鍵対応データを送出することを特徴とするもの。
【請求項７】請求項５または６の通信方法において、
前記重複期間の開始時点Ｔｓは、下式によって示されるものであることを特徴とするもの：
$Ts = Tx - Rmax - \alpha$
ここで、Txは暗号化データにおいて鍵の変わる時点、Rmaxは受信側において、前記重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、前記重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も大きな時間、αは余裕時間である。
【請求項８】請求項５、６または７の通信方法において、

前記重複期間の終了時点Teは、下式によって示されるものであることを特徴とするもの：

$Te = Tx - Rmin + \beta$

ここで、Txは暗号化データにおいて鍵の変わる時点、Rminは受信側において、前記重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、前記重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も小さな時間、βは余裕時間である。

【請求項９】所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する受信装置であって、

受け取った鍵対応データに基づいて、鍵を生成する鍵取得手段と、

受取手段によって受け取った暗号化データを、鍵取得手段によって取得した鍵に基づいて復号化する復号化手段であって、暗号化データに対する処理の開始時点において、１つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始する復号化手段と、

を備えた受信装置。

【請求項１０】請求項９の受信装置において、

前記２つの鍵に対応する鍵対応データは、現在の鍵に対応する鍵対応データと次の鍵に対応する鍵対応データとの２つの鍵対応データとして与えられ、前記１つの鍵に対応する鍵対応データは、現在の鍵に対応する１つの鍵対応データとして与えられており、

前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵に対応する１つの鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始し、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する２つの鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする受信装置。

【請求項１１】請求項１０の受信装置において、

前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する２つの鍵対応データを受けている場合には、現在の鍵を先に取得した際には、２つの鍵対応データが送信される期間の終了時点から鍵が変更される時点までの時間よりも、鍵対応データから次の鍵を取得する時間の方が短い場合には、次の鍵の取得を待たずに現在の鍵を取得した時点で、復号化したデータの出力を開始することを特徴とする受信装置。

【請求項１２】請求項９の受信装置において、

前記２つの鍵に対応する鍵対応データは、現在の鍵および次の鍵に対応する１つの鍵対応データとして与えられ、前記１つの鍵に対応する鍵対応データは、現在の鍵が１つの鍵対応データとして与えられており、

前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵に対応する１つの鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始し、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する１つの鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする受信装置。

【請求項１３】請求項１２の受信装置において、

前記復号化手段は、現在の鍵および次の鍵が含まれている１つの鍵対応データを受けた場合には、当該２つの鍵のうち、まだ復元していない次の鍵のみを復元するものであることを特徴とする受信装置。

【請求項１４】所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する受信装置であって、

暗号化データを鍵に基づいて復号化して出力する復号化出力部と、

復号化出力部の動作を制御する処理部と、

処理部の処理内容を定めたプログラムを記録している記録部と、

を備え、

前記プログラムは、処理部に接続された鍵復元部に鍵対応データを与えて鍵を復元させ、

復号化出力部において、受け取った暗号化データを、前記生成された鍵に基づいて復号化させるに際して、暗号化データに対する処理の開始時点において、１つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するよう制御するものであること、

を特徴とする受信装置。

【請求項１５】所定時間ごとに鍵を変えて暗号化された暗号化データを復号化する復号化装置であって、

暗号化データに対する処理の開始時点において、１つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するように構成されていることを特徴とする復号化装置。

【請求項１６】所定時間ごとに鍵を変えて暗号化された暗号化データを復号化する処理を制御するためのプログラムを記録した記録媒体であって、

当該プログラムは、受け取った鍵対応データに基づいて鍵を生成させ、
受け取った暗号化データを、前記生成された鍵に基づいて復号化させるに際して、暗号化データに対する処理の開始時点において、１つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するよう制御するものであること、
を特徴とするプログラムを記録した記録媒体。
【請求項１７】鍵対応データを受けて鍵を再生する鍵再生装置であって、
受け取った鍵対応データに対応する鍵の個数を検出する個数検出手段と、
当該個数検出手段によって検出された個数の鍵を、鍵対応データから再生する鍵再生手段と、
を備えたことを特徴とする鍵再生装置。
【請求項１８】所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する通信方法であって、
暗号化データと鍵対応データとを受け取り、
受け取った鍵対応データに基づいて鍵を生成し、
受け取った暗号化データを鍵に基づいて復号化するに際して、暗号化データに対する処理の開始時点において２つの鍵に対応する鍵対応データを受けている場合には、取得した現在の鍵に基づいて暗号化データを復号化するとともに取得した次の鍵を保持し、暗号化データに対する処理の開始時点において１つの鍵に対応する鍵対応データを受けている場合には、取得した鍵に基づいて暗号化データを復号化するようにしたことを特徴とする通信方法。
【請求項１９】請求項１８の通信方法において、
暗号化データに対する処理の開始時点において、１つの鍵に対応する鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始するようにしたことを特徴とする通信方法。
【発明の詳細な説明】
【０００１】
【発明の技術分野】この発明は暗号鍵による暗号化通信に関するものであり、特にその暗号鍵の伝送に関するものである。
【０００２】
【従来の技術】図３７に、従来の衛星デジタル放送受信機の構成をブロック図にて示す。衛星デジタル放送においては、画像データ、音声データ、制御データなどが、時分割のパケットとして送られてくる。また、このパケットは、暗号鍵によって暗号化されている。
【０００３】チューナ部２は、制御部４の制御に応じ、衛星から送信されてくる電波から、所望のトランスポートストリーム（周波数、偏波面などによって決定される伝送路）のパケット（ＴＳパケットと呼ぶ）を選択的に受信する。出力されたＴＳパケットには、複数のチャネルの画像データ、音声データ、制御データが時分割で含まれている。
【０００４】デ・スクランブル部６は、制御部４の制御に従って、暗号鍵に基づきＴＳパケットの暗号を解除する。さらに、デコーダ部８は、制御部４の制御に従って、ＴＳパケットから、所望のチャネルの画像データ、音声データ、制御データを選択的に取得する。ＮＴＳＣエンコーダ１０は、デコーダ部８によって得られた画像データ、音声データに基づいて、ＮＴＳＣコンポジット信号を生成する。
【０００５】ところで、放送局側から送られてくるＴＳパケットは、守秘性を高くするために、リアルタイムに暗号鍵を変えて伝送されてくるようになっている。その伝送状態を、図３８に示す。たとえば、図中のＴＳパケットにおいて、Odd0と表示された期間では、複数のＴＳパケットがOdd0の暗号鍵によって暗号化されている。同様に、Even1、Odd1、Even2の期間では、複数のＴＳパケットが、それぞれ、暗号鍵Even1、Odd1、Even2によって暗号化されている。
【０００６】ＴＳパケットの一部として、これら暗号鍵Odd0、Even1、Odd1、Even2自体を暗号化したＥＣＭデータも併せて送信されてくる。このＥＣＭデータは何度も繰り返し送信される。図３８は、ＥＣＭデータが繰り返し送信される期間を示している。
【０００７】図３８から明らかなように、ＴＳパケットにおいて現在用いられている暗号鍵のＥＣＭデータだけでなく、次に用いられる暗号鍵のＥＣＭデータも同時に送信されている。たとえば、図のT1のタイミングで受信を開始すると、デ・スクランブル部６は、受信したＥＣＭデータに基づいて、暗号鍵Odd0、Even1を復元する。この暗号鍵の復元にｔ1要するとすれば、T1＋ｔ1のタイミングから画像および音声が出力されることとなる。その後は、予め、次の暗号鍵が復元されて得られているので、とぎれることなく画像および音声が出力される。
【０００８】上記のように、常に、現在の暗号鍵と次の暗号鍵を取得することができるので、どのようなタイミングでチャネルの切替があっても、暗号鍵の復元時間ｔ1だけ待てば、画像および音声が得られる。
【０００９】また、図３９に示すようにして、暗号鍵のＥＣＭデータを伝送する方式もある。この方式では、ＴＳパケットに用いている暗号鍵のＥＣＭデータを、所定

時間Δｔだけ早く送信している。ＥＣＭデータから暗号鍵を復元するために要する時間よりも、このΔｔを大きくしておけば、とぎれることなく画像および音声を出力することができる。ＥＣＭデータから暗号鍵を復元するために要する時間は、受信機によって異なる。したがって、各種受信機においてＥＣＭデータから暗号鍵を復元するために要する時間のうち、最大の時間ｔmaxよりもΔｔが大きくなるように設定すれば、全ての受信機において、とぎれることなく画像および音声を得ることができる。

【００１０】

【発明が解決しようとする課題】上記のような従来の通信方式には、次のような問題点があった。

【００１１】図３８に示すような方式においては、２つの暗号鍵を１つのＥＣＭデータとして送るようにしているので、ＥＣＭデータが長くなって、ＥＣＭデータの送出のための時間が長くなるという問題点があった。また、ＥＣＭデータから暗号鍵を復元するための時間が長くなるという問題もあった。

【００１２】これに対し、図３９に示すような方式においては、１つの暗号鍵のみをＥＣＭデータとして送るようにしているので、ＥＣＭデータ送出のための時間が短く、暗号鍵復元に要する時間も短いという利点がある。

【００１３】しかしながら、暗号鍵復元に最も時間を要する受信機の復元時間ｔmaxを考慮してΔｔを設定しているので、チャネル切替時に、画像および音声が出力されるまでの時間がかかるという問題があった。図４０に、この問題点を説明するため、図３８の方式と図３９の方式とを比較して示す。ここで、タイミングＴ2において、チャネルが切り換えられて受信が開始されたとする。受信機が暗号鍵Odd0の復元に要する時間をｔ1とすれば、図３８の方式の場合には、Ｔ2＋ｔ1のタイミングから、画像および音声が得られることとなる。これに対し、図３９の方式の場合には、タイミングＴ2においては、もはや暗号鍵Odd0のECMデータが送られてきていないので、タイミングＴ3まで画像および音声が得られないこととなってしまう。このように、図３９の方式では、ＥＣＭデータ送出のための時間が短く、暗号鍵復元に要する時間も短いという利点があるものの、チャネル切り替え時などの受信開始時に、画像および音声が得られるまでの時間が長くなってしまうという問題があった。

【００１４】さらに、図３９の方式では、Δｔを、暗号鍵復元に最も時間を要する受信機の復元時間ｔmaxと等しくしておいても、チャネル切換時には、一旦表示された画像等が途切れるという現象が生じている。かかる現象については、経験上Δｔを大きくとることによって解決できることが分かっている。しかしながら、前述のように、Δｔをあまり大きくすると、復元処理の速い受信機においても、チャネル切換時に映像等が得られるまでの時間が長くなるという問題を生じる。そこで、従来、試行錯誤によって適切なΔｔの長さを決定しており、極めて煩雑であった。つまり、適切な結果を得るための通信パラメータの設定が困難であった。

【００１５】この発明は、上記のような問題点を解決して、暗号鍵送出のための占有時間が短く、かつ、受信開始時に、画像および音声が得られるまでの時間が短い通信システムおよび方法等を提供すること、並びにかかるシステムおよび方法において所望の結果を得るための通信パラメータの設定を容易にすることを目的とする。

【００１６】

【課題を解決するための手段および発明の効果】この発明に係る通信システムおよび方法は、所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出し、受信側において暗号化データを復号化する通信システムおよび方法であって、送信側においては、順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、暗号化データに用いた鍵が変わる時点より前の所定重複期間内において、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するとともに、受信側においては、送出されてきた暗号化データと鍵対応データとを受け取り、受け取った鍵対応データに基づいて鍵を生成し、受け取った暗号化データを鍵に基づいて復号化するに際し、暗号化データに対する処理の開始時点が前記重複期間以外の期間である場合は、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間である場合は、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴としている。

【００１７】上記のように、暗号化データに用いた鍵が変わる時点より前の所定重複期間においてのみ、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するようにしている。たとえば、重複期間において、当該時点での鍵に対応する鍵対応データと、次に使用する鍵に対応する鍵対応データとの２つの鍵対応データを送出するようにしたり、当該時点での鍵と次に使用する鍵とに対応する１つの鍵対応データを送出するようにしている。したがって、鍵対応データ送出のための占有時間を短くしつつ、受信開始時に、画像および音声が得られるまでの時間を短くすることができる。

【００１８】この発明では、重複期間の開始時点Tsが、下式によって示されるものであることを特徴としている。

【００１９】$Ts = Tx - Rmax - \alpha$

ここで、Txは暗号化データにおいて鍵の変わる時点、Rmaxは受信側において、重複期間外に受けた鍵対応データ

から鍵を取得するに必要な時間と、重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も大きな時間、αは余裕時間である。

【００２０】上記のようにRmaxを定めて重複期間の開始時点Tsを定めることにより、重複期間の始まる直前に処理を開始した場合であっても、途切れることなく復号化されたデータを得ることができる。また、想定した受信装置のうち、鍵対応データから鍵を復元する処理の最も遅い受信装置によってRmaxを定めているので、想定される全ての受信機において、これを達成することができる。また、処理開始時に途切れることなく復号化されたデータを得るために、重複期間の開始時期をどのように設定すればよいのかが明確となってシステム設計が容易となる。

【００２１】この発明では、重複期間の終了時点Teが、下式によって示されるものであることを特徴としている。

【００２２】$Te = Tx - Rmin + \beta$

ここで、Rminは受信側において、重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、重複期間内に受けた次の鍵に対応する鍵対応データから鍵を取得するに必要な時間とを合計した時間のうち想定した最も小さな時間、βは余裕時間である。

【００２３】現在使用する鍵が復元できた時点で、使用する鍵が次の鍵に変わっていた場合には、鍵の復元処理が無駄になる。そこで、想定した受信装置のうち、鍵対応データから鍵を復元する処理の最も速い受信装置に基づいて、重複期間の終了時点Teを、鍵の変化時点Txよりも前に終了させることにより、復元化されたデータの受信に支障を与えることなく重複期間を短くすることができる。

【００２４】この発明では、受信側での暗号化データの処理開始時点において、２つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するようにしている。したがって、処理開始の際に、復元化されたデータを途切れることなく受信することができる。

【００２５】この発明では、受信側での暗号化データの処理開始時点において、２つの鍵対応データを受けており、現在の鍵を先に取得した際には、２つの鍵対応データが送信される期間の終了時点から鍵が変更される時点までの時間よりも、鍵対応データから次の鍵を取得する時間の方が短い場合には、次の鍵の取得を待たずに現在の鍵を取得した時点で、復号化したデータの出力を開始することを特徴としている。したがって、処理の開始から復号化したデータの出力までの時間を、受信装置の処理速度に応じて短くすることができる。

【００２６】この発明では、２つの鍵が含まれている鍵対応データを受けた場合には、当該２つの鍵のうち、まだ復元していない鍵のみを復元するものであることを特徴としている。したがって、鍵の復元処理時間を短くすることができる。

【００２７】この発明において、「通信」とは、一斉放送、１対１通信等の形態を問わないものである。また、有線通信、無線通信を問わない。

【００２８】「受信装置」とは、暗号化されたデータを受けて、復号化して出力する機能を有する装置をいう。たとえば、衛星放送テレビジョンの電波を受信して、コンポジット信号として出力するセット・トップ・ボックス（ＳＴＢ）や、ＳＴＢの機能を内蔵したＴＶセットなどがこれに該当する。

【００２９】「鍵出力手段」とは、暗号化のための鍵を自ら生成する手段だけでなく、他の手段から受け取った鍵を保持して出力する手段も含む概念である。

【００３０】「復号化手段」とは、暗号化されたデータを受けて、これを鍵に基づいて復号化し、出力する手段をいう。実施形態においては、図１２のデ・スクランブラ６８、トランスポートデコーダ７０およびＣＰＵ７２（特に図１７、図２３、図３２、図３６に示す処理）が、これに対応する。

【００３１】「２つの鍵に対応する鍵対応データを受ける」とは、それぞれが１つの鍵に対応する鍵対応データを２つ受ける場合だけでなく、２つの鍵に対応する鍵対応データを１つ受ける場合をも含む概念である。実施形態では、前者は図１０に対応し、後者は図３１に対応する。

【００３２】「暗号化データに対する処理の開始時点」とは、当該暗号化データを復号化するために必要な鍵対応データを受け取った時点をいい、実施形態においては、図１８～図２２等の時点X1がこれに該当する。

【００３３】「送出すべきデータ」とは、暗号化して送信される対象となるデータであり、画像データ、音声データだけでなく、文書テキストデータ、プログラムデータ等であってもよい。

【００３４】「プログラムを記録した記録媒体」とは、ＣＰＵによって実行可能なプログラムを記録した、ＲＯＭ、ＲＡＭ、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ等の記録媒体をいう。また、プログラムは、ＣＰＵによって直接実行可能なものだけでなく、一旦インストールが必要なもの、圧縮されているもの、暗号化されているものも含まれる。

【００３５】

【発明の実施の形態】１．システムの全体構成

(1)システムのブロック図

この発明の一実施形態による通信システムの全体構成を図１に示す。この通信システムは、送信装置２０と受信装置２２を備えている。また、送信装置２０と受信装置３０とは、地上波通信、衛星通信、有線通信、ＷＡＮ、ＬＡＮ等の通信路（図示せず）によって結合されてい

る。

【００３６】送信装置２０は、鍵出力手段２２、暗号化手段２４、鍵対応データ生成手段２６、送出手段２８を備えている。鍵出力手段２２は、暗号化のための鍵を次々と生成する。暗号化手段２４は、送出すべきデータを鍵出力手段２２からの暗号鍵によって暗号化して、暗号化データを生成する。鍵対応データ生成手段２６は、鍵出力手段２２からの暗号鍵自体を暗号化して、鍵対応データを生成する。送出手段２８は、暗号化データとその暗号化に用いられた暗号鍵の鍵対応データとを送出する。

【００３７】受信装置３０は、受取手段３２、複合化手段３４、鍵取得手段３６を備えている。受取手段３２は、送信装置２０から送られてきた暗号化データおよび鍵対応データを受け取る。鍵取得手段３６は、受け取った鍵対応データから暗号鍵を復元する。複合化手段３４は、鍵取得手段３６によって復元された暗号鍵に基づいて、暗号化データを復号化してデータを取得して出力する。

【００３８】なお、図１においては、１つの送信装置に対して１つの受信装置を示している。しかしながら、この通信システムの適用分野によって、送信装置と受信装置の対応関係は異なったものとなる。たとえば、衛星放送システムに適用した場合には、１つの送信装置２０に対して、多くの受信装置３０が対応することとなる。また、受信装置３０が多くの衛星放送システムに対応している場合、受信装置３０の側から見れば、複数の送信装置２０に対して、１つの受信装置３０が対応することとなる。また、ＬＡＮなどのネットワーク通信に適用した場合には、複数の送信装置２０に対して、複数の受信装置３０が対応することとなる。

【００３９】(2)通信方法の概要

図１に示す通信システムにおける暗号化データと鍵対応データの送出タイミングを、図２に示す。鍵出力手段２２は、暗号鍵を順次出力する。ここでは、一連の暗号鍵をEven0,Odd0,Even1,Odd1,Even2....と表すこととする。Even0,Even1...を偶数鍵、Odd0,Odd1,Odd2....を奇数鍵という。暗号化手段２４は、送出すべきデータに対し期間を区切って、これら一連の暗号鍵によって暗号化を行って暗号化データを生成する。この状態を図２Ａに示す。

【００４０】送出手段２８は、暗号化データと鍵対応データを図２に示すようなタイミングにて送出する。なお、図２Ｂにおいて、Odd0,Even1,Odd1,Even2と示した部分は、それぞれ、暗号鍵Odd0,Even1,Odd1,Even2の鍵対応データを送出している期間であることを示している。また、各期間において、鍵対応データは、１回だけでなく複数回繰り返して同じものを送出するようにしている。これにより、鍵対応データの受信に失敗しても、再度、鍵対応データを受信して暗号鍵を得ることができる。

【００４１】図２Ｂに示すように、暗号化データにおいて用いた暗号鍵が変わる時点Txより$\Delta t1$だけ早く（Ts参照）、次の鍵対応データを送出している。

【００４２】これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、データが途切れることなく受信できるようにするためである。したがって、$\Delta t1$は、受信側の状況によって想定される暗号鍵復元時間のうち最悪の場合（最も時間がかかる場合）の時間を基準として、これと等しいかもしくは、わずかに大きいことが好ましい。複数の受信装置において最も復元の遅い装置の復元時間を基準としたり、１つの受信装置において処理負荷状況などによって変化する復元時間のうち最も遅いものを基準としたりすればよい。

【００４３】また、暗号化データの暗号化に現在用いられている暗号鍵の鍵対応データは、次の鍵対応データが送出され始めてからも、引き続き送出されている。したがって、この期間４０は、現在の鍵対応データと次の鍵対応データとが重複して送出されることとなる。この期間を重複期間と呼ぶ。現在の鍵対応データは、暗号鍵が変わる時点Txより$\Delta t2$だけ早い時点Teにおいて、送出が停止される。

【００４４】これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、不要な鍵対応データを送出しないようにするためである。つまり、鍵対応データから暗号鍵が復元できた時点において、すでに使用されている暗号鍵が次のものに変わっている場合には、その鍵対応データを送る必要はない。むしろ、鍵対応データを送ることによって、伝送路の実質的な伝送容量を低下させることとなる。したがって、$\Delta t2$は、受信側の状況によって想定される暗号鍵復元時間のうち最良の場合（最も時間がかからない場合）の時間を基準として、これと等しいかもしくは、わずかに小さいことが好ましい。複数の受信装置において最も復元の速い装置の復元時間を基準としたり、１つの受信装置において処理負荷状況などによって変化する復元時間のうち最も速いものを基準としたりすればよい。

【００４５】図２Ｂに示す重複期間４０を設けることにより、受信側における受信処理開始時でのデータ出力までの時間を、受信装置の性能や状況に応じて短くすることができる。つまり、いずれの受信装置においても、あるいは受信装置の処理状況がどのような状態にあっても、ほぼ、暗号鍵の復元時間経過後にデータの出力を得ることができる。

【００４６】２．衛星放送システムにおける第１の実施形態

次に、この発明による通信システムを衛星放送システムに適用した場合の実施形態について説明する。

【００４７】(1)送信装置の構成の説明

衛星放送においては、周波数や偏波方向などによって決

定される各トランスポンダのそれぞれに複数のチャネルが設定される。各トランスポンダにおいては、時分割によって複数チャネルのデータがパケット化されて送信されている。各トランスポンダによって伝送されるデータを、トランスポートストリームと呼ぶ。

【００４８】図３に、トランスポートストリームを生成して送信するための送信装置の構成を示す。図においては、１組の画像データ、音声データのみを示しているが、多数の画像データ、音声データの組が与えられる。音声データ、画像データの組は、所定個数ごとに１つのトランスポートストリームにまとめられる。

【００４９】画像データ４２は、画像エンコーダ４８によって圧縮されて多重化部５４に与えられる。同様に、音声データ４４は、音声エンコーダ５０によって圧縮されて多重化部５４に与えられる。なお、この実施形態では、MPEG2規格に基づいてデータの圧縮を行っている。

【００５０】制御データ生成部４６は、パケット化のための制御データを生成する。この制御データは、時分割された複数チャネルの画像データ、音声データを正しく識別するなどのために付される。多重化部５２は、制御データ、圧縮された画像データ、音声データおよび後述するＥＣＭデータを時分割して固定長のパケットにし、トランスポートストリームとして出力する。この際、多重化部５４は、誤り訂正の符号を付加する。この実施形態では、畳み込み符号化を内符号、短縮化リードソロモン符号を外符号とする連接符号によって、誤り訂正を行っている。

【００５１】スクランブラ５６は、出力されたパケットに対し、スクランブル鍵制御部６０から与えられるスクランブル鍵を用いてスクランブルをかける。スクランブルのかけられたトランスポートストリームは、変調部５８において変調され、放送衛星を介して視聴者に放送される。

【００５２】なお、スクランブラ５６において用いられたスクランブル鍵は、ＥＣＭ生成部５２において暗号化され、鍵対応データであるＥＣＭ(Entitlement Control Message)データとされる。多重化部５４は、このＥＣＭデータも含めてパケット化する。

【００５３】この実施形態においては、エネルギー拡散方式を用いて、M系列により発生する疑似ランダム信号を加算することにより、スクランブルをかけるようにしている。なお、この他の暗号化方式によってスクランブルをかけるようにしても良い。

【００５４】(2)トランスポートストリームの構造

図３の送信装置によって生成されたトランスポートストリームの構造を説明する。この実施形態では、パケット化の制御データとして、MPEG2システムに規定されるＰＳＩ(Program Specific Information)を用いている。

【００５５】図４を参照して、３つのチャネルを時分割多重化したトランスポートストリームの構造を説明する。画像データはES(Video)1,ES(Video)2,ES(Video)3として示され、音声データはES(Audio)1,ES(Audio)2,ES(Audio)3として示されている。ECM1は画像データES(Video)1、音声データES(Audio)1に用いたスクランブル鍵のＥＣＭデータを示している。同様に、ECM2は画像データES(Video)2、音声データES(Audio)2に用いたスクランブル鍵のＥＣＭデータを示し、ECM3は画像データES(Video)3、音声データES(Audio)3に用いたスクランブル鍵のＥＣＭデータを示している。

【００５６】NIT,PAT,PMT1,PMT2,PMT3は、ＰＳＩによるパケット化における制御データである。これらの制御データにより、各トランスポートストリームに含まれるチャネル、時分割多重化されパケット化された３つのチャネルの画像データ、音声データを識別することができる。制御データNIT,PAT,PMT1,PMT2,PMT3のデータ構造は、後に詳述する。

【００５７】パケット化は、図４の縦線６０ａに示すように行われる。つまり、制御データNIT,PAT,PMT1,PMT2,PMT3、ＥＣＭデータECM1,ECM2,ECM3、画像データES(Video)1,ES(Video)2,ES(Video)3、音声データES(Audio)1,ES(Audio)2,ES(Audio)3の順にパケット化が行われる。音声データES(Audio)3までのパケット化が完了すれば、再び、制御データNIT以下のパケット化を繰り返す（縦線６０ｂ参照）。

【００５８】画像データES(Video)1,ES(Video)2,ES(Video)3や音声データES(Audio)1,ES(Audio)2,ES(Audio)3は、制御データやＥＣＭデータに比べて大量に送られる。この実施形態では、固定長パケットを用いているので、画像データES(Video)1,ES(Video)2,ES(Video)3や音声データES(Audio)1,ES(Audio)2,ES(Audio)3は、制御データやＥＣＭデータに比べて多くのパケットが送られることとなる。図４において、画像データおよび音声データが太く示されているのは、このことを模式的に表したものである。

【００５９】図５に、パケット化されたデータの基本的構造を示す。制御データ、ＥＣＭデータ、画像データ、音声データのいずれもが、図５に示すようなデータ構造を持つパケットとされる。パケット化データの先頭には、パケット符号PID(Packet ID)が付される。パケット符号PIDは、各パケットを識別するため各パケットごとにユニークに付された符号である。スクランブルコントロールビットは、当該パケットにスクランブルがかかっているか否か、スクランブルがかかっている場合には偶数鍵(Even)か奇数鍵(Odd)かを示す。たとえば、"00"はスクランブル無し、"10"は偶数鍵によるスクランブル、"11"は奇数鍵によるスクランブルを示す。内容データは、パケット化された対象データ（制御データ、ＥＣＭデータ、画像データ、音声データなど）である。

【００６０】なお、この実施形態では、制御データNIT,PAT,PMT1,PMT2,PMT3やＥＣＭデータECM1,ECM2,ECM3にス

クランブルをかけないようにしている。したがって、これらデータのパケットにおいて、スクランブルコントロールビットは"00"となる。

【００６１】図６に制御データPATのデータ構造を示し、図７に制御データPMT1,PMT2,PMT3のデータ構造を示す。制御データPMT1は、図７に示すように、画像データES(Video)1のパケット符号PIDとそのスクランブル鍵のＥＣＭデータECM1のパケット符号PID、および音声データES(Audio)1のパケット符号PIDとそのスクランブル鍵のＥＣＭデータECM1のパケット符号PIDを有している。図７においては、画像データのＥＣＭデータのPIDが１６進数で２１、画像データのPIDが１６進数で２２、音声データのＥＣＭデータのPIDが１６進数で２１、音声データのPIDが１６進数で２４であることが示されている。なお、他のチャンネルの制御データPMT2,PMT3も同様の構成である。また、この実施形態では、画像データと音声データのスクランブル鍵を同じものとしたが、それぞれ異なるスクランブル鍵を用いるようにしてもよい。

【００６２】制御データPATは、図６に示すように、各チャネルの制御データPMT1,PMT2,PMT3のパケット符号PIDを示している。図６においては、３チャネルのPMTのPIDが１６進数で１０、５チャネルのPMTのPIDが１６進数で１１、７チャネルのPMTのPIDが１６進数で１２であることが示されている。

【００６３】図６、図７に示す制御データPAT、PMTによって、画像データ、音声データのパケットが、チャネルごとに特定できる。

【００６４】図８にＥＣＭデータECM1,ECM2,ECM3の構造を示す。ＥＣＭデータは、セクションヘッダとＥＣＭ内容データとを有している。ＥＣＭ内容データは、スクランブル鍵自体を暗号化したものである。セクションヘッダには、偶数鍵(Even)か奇数鍵(Odd)かを示すtable_id、このＥＣＭデータによるスクランブル鍵が現在の鍵（カレント鍵という）か、次に用いる鍵（ネクスト鍵という）かを示すtable_id_extensionが設けられている。この実施形態では、table_idが８進数で８２であれば偶数鍵であること、８３であれば奇数鍵であることを表す。また、table_id_extensionが００であれば、このＥＣＭデータがカレント鍵のものでありカレント鍵だけが送られていること、０１であれば、このＥＣＭデータがカレント鍵のものであり同時にネクスト鍵も送られていること、１０であれば、このＥＣＭデータがネクスト鍵のものであることを表している。

【００６５】なお、この実施形態では、table_id_extensionによって上記の区別を行っている。しかしながら、ＥＣＭデータの内容に、このような区別を行うデータを記述するようにしてもよい。

【００６６】以上のようにして、１つのトランスポンダに複数のチャネルのデータが時分割で多重化され、１つのトランスポートストリームを形成している。なお、トランスポートストリームは複数設けられており、図９に示すようにその識別子Ts_id、周波数・偏波方向などの伝送諸元、そのトランスポートストリームに含まれるチャネルのリストがNIT(Network Information Table)データとして伝送される。

【００６７】図１０に、画像データES(Video)1（または音声データES(Audio)1）とＥＣＭデータECM1の送出タイミングを示す。なお、図１０の画像（音声）データにおいて、Odd0,Even1,Odd1,Even2と示した部分は、それぞれ、スクランブル鍵Odd0,Even1,Odd1,Even2によってスクランブルをかけた部分である。また、ＥＣＭデータECM1において、Odd0,Even1,Odd1,Even2と示した部分は、それぞれ、スクランブル鍵Odd0,Even1,Odd1,Even2の鍵対応データを送出している期間であることを示している。なお、他のチャネルの画像データES(Video)2,ES(Audio)2とＥＣＭデータECM2とのタイミング関係、画像データES(Video)3,ES(Audio)3とＥＣＭデータECM3とのタイミング関係も、上記と同様である。

【００６８】図４においては、ＥＣＭデータは１本のデータとして示されているが、より詳細には、図１０に示すように、所定の重複期間では２つのＥＣＭデータが同時に送られている。図１１に、重複期間の前後を拡大して示す。図１１に示すように、画像（音声）データにおいて用いたスクランブル鍵がOdd0からEven1へ変わる時点Txより$\Delta t1$だけ早いタイミングTsにて、次のスクランブル鍵Even1の鍵対応データを送出している。

【００６９】これは、受信装置において、鍵対応データからスクランブル鍵を復元するための時間を考慮して、画像や音声が途切れることなく受信できるようにするためである。したがって、重複期間４０の開始時Tsは下式のように定めるのが好ましい。

【００７０】$Ts = Tx - Rmax - \alpha$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rmaxは、最大復元時間であり、想定される複数の受信装置において、連続して２つのＥＣＭデータを受けた時に、２つのスクランブル鍵に復元するために要する２重復元時間のうち、最も大きいものをいう。αは余裕時間であり、０と等しいかそれ以上の値を持つ。

【００７１】図１５Ａに示すように、１つずつしか復元処理をしない受信装置を想定する場合には、時点Q1から時点Q2までを２重復元時間とし、想定した各受信装置の２重復元時間のうち最も大きいものを最大復元時間Rmaxとする。

【００７２】また、図１５Ｂに示すように、２つの復元処理を並列して行う受信装置を想定する場合には、２つのＥＣＭデータを同時に与えてからスクランブル鍵を復元できるまでを２重復元時間とし、想定した各受信装置の２重復元時間のうち最も大きいものを最大復元時間Rmaxとする。

【００７３】さらに、図１５Ａ、図１５Ｂのような受信装置が混在することが想定される場合には、それぞれの最大復元時間のうち最も大きいものを全体としての最大復元時間Rmaxとする。

【００７４】図１１に戻って、暗号化データの暗号化に現在用いられているスクランブル鍵Odd0の鍵対応データは、次の鍵Even1の鍵対応データが送出され始めてからも、引き続き送出されている。したがって、この期間４０は、現在の鍵Odd0の鍵対応データと次の鍵Even1の鍵対応データとが重複して送出されることとなる。現在の鍵Odd0の鍵対応データは、スクランブル鍵が変わる時点Txより$\Delta t2$だけ早い時点Teにおいて、送出が停止される。

【００７５】これは、受信側において、鍵対応データからスクランブル鍵を復元するための時間を考慮して、不要な鍵対応データを送出しないようにするためである。つまり、鍵対応データからスクランブル鍵Odd0が復元できた時点において、すでに使用されているスクランブル鍵が次のものEven1に変わっている場合には、その鍵対応データを送る必要はない。むしろ、鍵対応データを送ることによって、伝送路の実質的な伝送容量を低下させることとなる。したがって、重複期間４０の終了時Teは下式のように定めるのが好ましい。

【００７６】$Te = Tx - Rmin + \beta$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rminは最小復元時間であり、想定される複数の受信装置において、連続して２つのＥＣＭデータを受けた場合に、２つのスクランブル鍵に復元するために要する２重復元時間のうち、最も小さいものをいう。βは余裕時間であり、０と等しいかそれ以上の値を持つ。

【００７７】図１５Ａに示すように、１つずつしか復元処理をしない受信装置を想定する場合には、時点Q1から時点Q2までを２重復元時間とし、想定した各受信装置の２重復元時間のうち最も小さいものを最小復元時間Rminとする。

【００７８】また、図１５Ｂに示すように、２つの復元処理を並列して行う受信装置を想定する場合には、２つのＥＣＭデータを同時に与えてからスクランブル鍵を復元できるまでを２重復元時間とし、想定した各受信装置の２重復元時間のうち最も小さいものを最小復元時間Rminとする。

【００７９】さらに、図１５Ａ、図１５Ｂのような受信装置が混在することが想定される場合には、それぞれの最小復元時間のうち最も小さいものを全体としての最小復元時間Rminとする。

【００８０】なお、RmaxやRminを決定するために想定する受信装置として、可能性のある全ての受信装置を想定した場合には、全受信装置においてチャネル切換時の画像等の乱れを防止することができる。しかし、全受信装置に対して所定の割合（９５％等）のものについて、チャネル切換時の画像等の乱れを防止することができるように受信装置を想定し、RmaxやRminを決定してもよい。

【００８１】(3)受信装置の構成

図１２に、この実施形態による通信システムにおける受信装置のブロック図を示す。この実施形態においては、復調部６４が受取手段３２に該当し、ＩＣカード８０が鍵取得手段３６に該当する。また、デ・スクランブラ６８、トランスポートデコーダ７０およびＣＰＵ７２によって復号化手段３４を実現している。

【００８２】アンテナ６２によって受信された電波は、復調部６４において選択され、所望のトランスポートストリームのみがデジタルデータとして取り出される。誤り訂正部６６は、パケットに付されている誤り訂正符号に基づいてデータの誤り訂正を行う。

【００８３】デ・スクランブラ６８は、スクランブル鍵に基づいて、トランスポートストリームのスクランブルを解除する。なお、パケットの中には制御データやＥＣＭデータのパケットようにスクランブルがかけられていないものも含まれる。スクランブルがかかっていないパケットの場合、デ・スクランブラ６８は、何も処理を行わずそのままそのパケットを出力する。なお、スクランブルがかかっているか否かは、パケットのスクランブルコントロールビット（図５参照）を見ることにより判断することができる。

【００８４】図１３に、デ・スクランブラ６８内に設けられているＤＳレジスタを示す。デ・スクランブラ６８は、ＣＰＵ７２から与えられたスクランブル鍵と、そのスクランブル鍵を用いてスクランブルをかけられたパケットの符号PIDを、このＤＳレジスタに記憶する。なお、スクランブル鍵は、偶数鍵（Even鍵）と奇数鍵（Odd鍵）の２つが記憶されるようになっている。

【００８５】デ・スクランブラ６８は、与えられたパケットのスクランブルコントロールビット（図５参照）に基づいて、スクランブルされているか否かを判断する。スクランブルされていない場合には、誤り訂正部６６からのトランスポートストリームをそのままトランスポートデコーダ７０に与える。また、偶数鍵によってスクランブルされている場合には、当該パケットの偶数鍵をＤＳレジスタによって知り、その偶数鍵によってスクランブルを解除する。スクランブルの解除されたトランスポートストリームは、トランスポートデコーダ７０に与えられる。奇数鍵によってスクランブルされている場合も同様である。

【００８６】また、ＤＳレジスタに必要なスクランブル鍵が記憶されていない場合（図のPIDが0x75であるパケットに対する偶数鍵を参照）には、スクランブルを解除することができないので、スクランブルされたままトランスポートデコーダ７０に与える。

【００８７】トランスポートデコーダ７０は、デ・スクランブラ６８からトランスポートストリームを受け、処

理部であるＣＰＵ７２によって指定されたPIDを持つパケットのみを取り出す。この実施形態では、デ・スクランブラ６８とトランスポートデコーダ７０によって復元出力部が構成されている。

【００８８】取り出されたパケットの内、画像データ、音声データは、ビデオデコーダ８２、オーディオデコーダ８４において圧縮が解凍され、アナログ信号に変換されて出力される。画像信号は、ＣＲＴコントローラ８６によりＮＴＳＣ画像信号に変換されて出力される。

【００８９】ＣＲＴコントローラ８６からのＮＴＳＣ画像信号と、オーディオデコーダ８４からの音声信号は、ＴＶセット８８に与えられる。したがって、ＴＶセットのディスプレイ（図示せず）から画像が、スピーカ（図示せず）から音声が出力される。

【００９０】この実施形態では、受信装置本体９０の出力はＴＶセット８８に与えられている。しかしながら、アナログビデオレコーダ、デジタルビデオレコーダ、パーソナルコンピュータ等の他の機器に与えるようにしてもよい。パーソナルコンピュータやデジタルビデオデコーダ等のデジタル機器に出力する場合には、ビデオデコーダ８２、オーディオデコーダ８４において解凍した後のデジタルデータを与えるようにする。

【００９１】トランスポートデコーダ７０において取り出されたデータの内、制御データやＥＣＭデータは、記憶部であるメモリ７４に記憶される。ＥＣＭデータはＣＰＵ７２によって、コネクタ７９を介して復元処理部であるＩＣカード８０に送られ、ＩＣカード８０はこのＥＣＭデータからスクランブル鍵を復元する。復元されたスクランブル鍵は、コネクタ７９を介してＣＰＵ７２に送り返される。ＣＰＵ７２は、これをデ・スクランブラ６８に与える。なお、メモリ７４には制御プログラムも格納されている。ＣＰＵ７２は、この制御プログラムにしたがって、各部を制御する。

【００９２】操作パネル７８は、操作者の操作により、チャネル情報の入力等を行うためのものである。リモコン受光部７６は、リモコン（図示せず）から送られてきたチャネル情報等を受けるためのものである。

【００９３】リモコン受光部７６、操作パネル８６からのチャネル情報はＣＰＵ７２に与えられる。ＣＰＵ７６はチャネル情報を復調部６４に与え、所望のチャネルが属するトランスポートストリームのみを復調させる。また、受信した制御データに基づいて、トランスポートデコーダ７０により、トランスポートストリームから所望のチャネルのデータのみを取り出させる。

【００９４】図１４に、鍵取得手段であるＩＣカード８０の構成を示す。このＩＣカード８０は、受信装置本体９０と接続するためのコネクタ９４、データ伝送のためのインターフェイス９６、ＣＰＵ９２、メモリ９８を備えている。ＣＰＵ９２は、メモリ９８に格納されたプログラムにしたがって、コネクタ９４、インターフェイス９６を介して受け取ったＥＣＭデータに基づいてスクランブル鍵を復元する。

【００９５】この実施形態におけるＩＣカード８０は、一度に１つのＥＣＭデータに対する復元処理を行う（図１５Ａ参照）。したがって、ＣＰＵ７２は、ＥＣＭデータをＩＣカード８０に送った後、ＩＣカード８０からスクランブル鍵が返送されて来るのを待って、次のＥＣＭデータをＩＣカード８０に送るようにしている。

【００９６】(4)受信装置の動作

①鍵復元を１つずつ行う場合

図１６、図１７に、メモリ７４に記憶された制御プログラムのフローチャートを示す。この制御プログラムは、受信装置本体９０の電源投入またはチャネルの切換により処理を開始する。以下、このフローチャートを参照しつつ受信装置の動作を説明する。

【００９７】まず、ステップＳ１において、ＣＰＵ７２は電源投入であるかチャネル切換であるかを判断する。操作パネル７８またはリモコン受光部７６より新たなチャネル情報（所望のチャネルを示す情報）が与えられた場合には、チャネル切換であると判断できる。また、リセット動作が行われることにより、電源投入であると判断できる。

【００９８】チャネル切換であった場合には、現在受信しているトランスポートストリームに所望のチャネルが含まれているかどうかを判断する。この判断は、受信した制御データNITの内容を見ることによって行うことができる（図４および図９参照）。

【００９９】現在受信中のトランスポートストリーム内に所望のチャネルが含まれていない場合、ＣＰＵ７２は、図９に示す制御データNITの内容にしたがって所望のチャネルが含まれるトランスポートストリームの識別子Ts_id、伝送諸元を取得する。ＣＰＵ７２は、取得したトランスポートストリームの識別子Ts_id、伝送諸元を復調部６４に与える（ステップＳ３）。復調部６４は、与えられた識別子Ts_id、伝送諸元にもとづいて、所望のトランスポートストリームのみを選択的に復調して出力する。これにより、誤り訂正部６６によって誤り訂正されたトランスポートストリームが、デ・スクランブラ６８に与えられる。ＣＰＵ７２は、ステップＳ４の処理に進む。

【０１００】なお、現在受信しているトランスポートストリーム内に所望のチャネルが含まれている場合には、復調部６４の切換を行う必要がないので、ＣＰＵ７２は、ただちにステップＳ４の処理に進む。

【０１０１】また、電源投入の場合には現在受信中のトランスポートストリームが存在しないので、ＣＰＵ７２は復調部６４の切換を行った後、ステップＳ４の処理に進む。

【０１０２】ステップＳ４において、ＣＰＵ７２は、トランスポートデコーダ７０に、制御データPATのパケッ

ト符号PIDを設定する。これにより、トランスポートデコーダ７０は、トランスポートストリームから制御データPATを取り出して、メモリ７４に記憶する。

【０１０３】次に、ＣＰＵ７２は、メモリ７４に記憶された制御データPATに基づいて、所望のチャネルの制御データPMTのパケット符号PIDを取得する（図６参照）。図６の例でいえば、３チャネルを受信するのであれば、３チャネルの制御データPMTのパケット符号PIDが１６進数で”１０”であることがわかる。

【０１０４】続けて、ＣＰＵ７２は、トランスポートデコーダ７０に、所望のチャネルの制御データPMTのパケット符号PIDを設定する。これにより、トランスポートデコーダ７０は、トランスポートストリームから所望のチャネルの制御データPMTを取り出して、メモリ７４に記憶する。

【０１０５】さらに、ＣＰＵ７２は、メモリ７４に記憶された制御データPMTに基づいて、所望のチャネルの画像データ、音声データ、ＥＣＭデータのパケット符号PIDを取得する（図７参照）。ＣＰＵ７２は、取得したパケット符号PIDに基づいて、画像データ、音声データを取得するようにトランスポートデコーダ７０を制御し、ＥＣＭデータからスクランブル鍵を復元させるようにＩＣカード８０を制御し、スクランブル鍵によって画像データ、音声データのスクランブルを解除するようにデ・スクランブラ６８を制御する（ステップＳ６）。

【０１０６】ステップＳ６における処理の詳細を図１７に示す。ここでは、図１８の時点Ｘ１において、チャネルの切換または電源投入があって、このチャネルに対する処理が開始されたものとして説明を進める。

【０１０７】まず、所望のチャネルの画像、音声データのスクランブル鍵に対応するＥＣＭデータのパケット符号ＰＩＤを、トランスポートデコーダ７０に設定する（ステップＳ１１）。これにより、トランスポートデコーダ７０は、設定されたPIDを持つＥＣＭデータ（つまり所望のチャネルの画像、音声データのスクランブル鍵のＥＣＭデータ）を選択的に取り出してメモリ７４に記憶する。

【０１０８】さらに、ＣＰＵ７２は、取得したＥＣＭデータのtable_idおよびtable_id_extensionを読んで、必要としているＥＣＭデータであるか否かを判断する（ステップＳ１１）。このような判断を行うのは、一度取得したＥＣＭデータはもはや取得する必要がないので、新たなＥＣＭデータのみを取得するようにするためである。具体的には、必要とするＥＣＭデータのtable_id、table_id_extensionを指定することによってこの判断を行うが、その詳細については後述する。なお、処理開始時には、必要とするＥＣＭデータのtable_id、table_id_extensionの指定は行わないので、パケット符号PIDによって指定したＥＣＭデータであれば、無条件で指定条件を満たしたものとみなされる。

【０１０９】指定条件を満たさないＥＣＭデータである場合には、再び、ＥＣＭデータの取得を繰り返す。指定条件を満たすＥＣＭデータである場合には、当該ＥＣＭデータをＩＣカード８０に送る（ステップＳ１２）。つまり、図１８の時点X1において、スクランブル鍵Odd0のＥＣＭデータをＩＣカード８０に送る。ＥＣＭデータを受け取ったＩＣカード８０は、このＥＣＭデータからスクランブル鍵Odd0を復元し、時点X2においてＣＰＵ７２に送り返す（ステップＳ１３）。

【０１１０】スクランブル鍵Odd0を受け取ったＣＰＵ７２は、スクランブル鍵Odd0をデ・スクランブラ６８に設定する。これにより、デ・スクランブラ６８は、画像および音声データのスクランブルを解除してトランスポートデコーダ７０に出力するようになる。

【０１１１】ECMデータには、図８に示すようにtable_id_extensionとして、カレントのみ、カレント（ネクスト有り）、ネクストの３つの区別が付されている。これにより、CPU７２は、受け取った鍵が、図１０のａの期間（カレントのみ）にあるのか、ｂの期間（カレント（ネクスト有り））にあるのか、ｃの期間（ネクスト）にあるのかを知ることができる。なお、ｄに示す期間は、Even1鍵にとって、本来、ネクストとすべきであるが、この実施形態ではカレントとして扱っている。

【０１１２】ＣＰＵ７２は、table_id_extensionに基づいて、ＩＣカード８０から受け取った鍵がカレント鍵（現在使われている鍵）であるか、ネクスト鍵（次に使われる鍵）であるかを判断する（ステップＳ１５）。スクランブル鍵Odd0のＥＣＭデータのtable_id_extensionには、カレント鍵である旨の区別が付されているので、ＣＰＵ７２はステップＳ１６に進む。

【０１１３】ステップＳ１６においては、X1の時点において、ネクスト鍵が同時に送られてきていたか否かを判断する。これも、スクランブル鍵Odd0のＥＣＭデータのtable_id_extensionによって判断することができる。時点X1においては、カレント鍵のみであって、ネクスト鍵はまだ送信されていないことがtable_id_extensionよりわかるので、ステップＳ１７に進む。ステップＳ１７においては、トランスポートデコーダ７０に、所望のチャネルの画像データ、音声データのパケット符号ＰＩＤが設定されているかどうかを判断する。現在、まだ画像データ、音声データのＰＩＤは設定していないので、ステップＳ１８に進む。

【０１１４】ステップＳ１８において、ＣＰＵ７２は、すでにステップＳ５において取得している所望のチャネルの画像データ、音声データのパケット符号PIDを、トランスポートデコーダ７０に設定する。これにより、トランスポートデコーダ７０は、所望のチャネルの画像データ、音声データを、ビデオデコーダ８２、オーディオデコーダ８４に出力し始める。すなわち、図１８の場合には、時点X1にてチャネル切換が行われてから、ＩＣカ

ード８０による復元処理時間経過後の時点X2より、画像および音声がＴＶセット８８から出力される。時点X1にチャネル切換があれば、時点X2において、画像・音声が立ち上がる。

【０１１５】次に、ＣＰＵ７２は、ステップＳ１１における受信すべきＥＣＭデータの設定を変更する（ステップＳ１９）。これは、現在の鍵Odd0は既に取得したので、次の鍵Even1を取得ように設定するためである。ここでは、今回取得したＥＣＭデータと異なったtable_id（つまり偶数鍵）を持ったＥＣＭデータを取得するよう設定する。なお、table_idは、図８に示すように、偶数鍵、奇数鍵によって異なるようになっている。その後、ステップＳ１１に戻って処理を繰り返す。

【０１１６】この実施形態では、table_idによって、すでにその鍵を取得したかどうかを判断するようにしているが、セクションヘッダ中のバージョン情報によって判断するようにしてもよい。この場合、異なるＥＣＭデータには、異なるバージョン情報を付しておくようにする。

【０１１７】次に、ネクスト鍵Even1のＥＣＭデータを取得すると（ステップＳ１２、図１８の時点X3）、ＩＣカード８０によってネクスト鍵Even1を得る（ステップＳ１３、時点X4）。ＣＰＵ７２は、これをデ・スクランブラ６８に設定する（ステップＳ１４）。このようにして、ネクスト鍵Even1によってスクランブルされた画像データ、音声データが送られてくる前に、ネクスト鍵Even1をデ・スクランブラ６８に設定するので、画像および音声データを途切れることなく出力することができる。

【０１１８】次に、ＣＰＵ７２は、トランスポートデコーダ７０に、画像データ、音声データのＰＩＤが設定されているか否かを判断する（ステップＳ２０）。ここでは、すでにＰＩＤが設定されているので、ステップＳ２１に進んで、取得するＥＣＭデータの設定を変更する。

【０１１９】ステップＳ２１においては、今回取得したＥＣＭデータと異なったtable_idを持ち、ネクストのtable_id_extensionを持ったＥＣＭデータを取得するよう設定する。その後、ステップＳ１１に戻って処理を繰り返す。

【０１２０】以後は、順次上記の処理を繰り返して、ＴＶセット８８にＮＴＳＣ画像信号と音声信号を出力する。

【０１２１】なお、図１９に示すように、チャネル切換の時点X1が重複期間４０の開始時点に近接している場合には、ネクスト鍵Even1のＥＣＭデータが送られてきていても、ＩＣカード８０がカレント鍵Odd0の復元処理を行っている状態となる。したがって、ネクスト鍵Even1の復元処理は、カレント鍵Odd0の復元処理が終わってから（時点X2,X3参照）ということになり、ネクスト鍵Even1の取得が後ろにずれ込むこととなる。

【０１２２】しかしながら、図１９のΔt1は、最も遅い処理の受信装置における２重復元時間（２つのＥＣＭデータから連続して２つのスクランブル鍵を復元するに要する時間）を基準として設定されているので、スクランブル鍵が変わる時点Txよりも早くネクスト鍵Even1をデ・スクランブラ６８に設定することができる。つまり、画像および音声が途切れることなく出力される。したがって、図１９に示す場合も、図１８と同じように、時点X1にてチャネル切換が行われてから、ＩＣカード８０による復元処理時間経過後の時点X2に、画像および音声が立ち上がる。つまり、画像および音声をＴＶセット８８から得ることができる。

【０１２３】次に、図２０に示すように、時点X1においてチャネルの切換または電源投入があって、このチャネルに対する処理が開始された場合の処理を説明する。時点X1は重複期間４０内にあるので、カレントの鍵Odd0のＥＣＭデータとネクストの鍵Even1のＥＣＭデータが送られてきている。

【０１２４】ＣＰＵ７２は、取得したＥＣＭデータのtable_id_extensionから、そのＥＣＭデータによる鍵が、カレント鍵（ネクストあり）か、ネクスト鍵かを判断することができる（図８参照）。先に、時点X1において、カレント鍵Odd0のＥＣＭデータを取得した場合には、時点X2においてカレント鍵Odd0をＩＣカード８０から得る。ＣＰＵ７２は、当該カレント鍵Odd0をデ・スクランブラ６８に設定した後、ステップＳ１５を経て、ステップＳ１６に進む。ここでは、（ネクストあり）であるから、ステップＳ１９に進んで、取得するＥＣＭデータの設定を変更する。ここでは、異なるtable_idのＥＣＭデータ（つまり偶数鍵のＥＣＭデータ）を指定し、ステップＳ１１以下を実行する。

【０１２５】指定した偶数鍵（つまりネクスト鍵Even1）のＥＣＭデータを取得すると（時点X3）、これをＩＣカード８０に送って、ネクスト鍵Even1を得る（時点X4）。ＣＰＵ７２は、これをデ・スクランブラ６８に設定する（ステップＳ１４）。次に、ステップＳ１５を経て、デコーダ７０に音声・画像のＰＩＤを設定済みかどうかを判断する（ステップＳ２０）。ここではまだ設定していないので、ステップＳ１８に進み、所望のチャネルの画像データ、音声データのパケット符号PIDをトランスポートデコーダ７０に設定し、デコードを開始する。つまり、図２０の場合には、時点X1のチャネル切換に対し、時点X4から画像、音声が立ち上がる。

【０１２６】上記のように、重複期間４０内においてチャネル切換等によって当該チャネルに対する処理を開始した場合には、カレント鍵だけが取得できた時点X2ではデコードを開始せず（ＰＩＤを設定せず）、ネクスト鍵が得られてはじめてデコードを開始し（ＰＩＤを設定し）、画像データ、音声データを出力するようにしている。

【０１２７】上記のように処理している理由を、図２１を用いて説明する。図２１に示すような場合において、カレント鍵Odd0だけが取得できた時点X2からデコードを開始すると、区間R1で画像・音声が得られた後、区間R2で画像・音声が途切れるという問題を生じる。これは、区間R2ではネクスト鍵Even1がまだ取得できていないためである。

【０１２８】したがって、重複期間４０内において当該チャネルの処理を開始した場合には、ネクスト鍵が得られてから音声・画像のＰＩＤをデコーダ７０に設定するようにしている。その結果、図２１の場合であれば、時点X4から画像・音声出力が得られることとなり、画像や音声の途切れがない。

【０１２９】なお、図２０の場合において、時点X1で先にネクスト鍵Even1のＥＣＭデータを取得し、時点X2でネクスト鍵Even1が得られた場合には、ステップＳ１５、Ｓ２０を経て、トランスポートデコーダ７０に画像および音声のパケット符号PIDを設定する（ステップＳ１８）。つまり、カレント鍵Odd0の取得を待たずに、デコーダ７０への設定を行う。しかし、ネクスト鍵Even1によってスクランブルされた画像および音声データはまだ送られてきていないので、設定したパケット符号PIDに対応する画像および音声データが直ちに出力されるものではない。

【０１３０】その後、時点X4にてカレント鍵Odd0を取得した時点で、現在送られてきている画像および音声データのスクランブルを解除することができ、画像および音声が出力される。したがって、結果的に、時点X4から画像および音声が得られる点は同じである。

【０１３１】また、図２１の場合において、時点X1で先にネクスト鍵Even1のＥＣＭデータを取得し、時点X2でネクスト鍵Even1が得られた場合には、ステップＳ１５、Ｓ２０を経て、トランスポートデコーダ７０に画像および音声のパケット符号PIDを設定する（ステップＳ１８）。つまり、カレント鍵Odd0の取得を待たずに、デコーダ７０への設定を行う。しかし、ネクスト鍵Even1によってスクランブルされた画像および音声データはまだ送られてきていないので、設定したパケット符号PIDに対応する画像および音声データが直ちに出力されるものではない。

【０１３２】その後、ネクスト鍵Even1によってスクランブルがかけられた画像および音声データが送られてくる時点Txより、画像および音声データが出力されることとなる。なお、このケースの場合には、時点X4にて復元されたOdd0鍵は使用されない。

【０１３３】いずれにしても、この実施形態では、重複期間４０においてチャネル切換等によって処理を開始した場合、少なくともネクスト鍵が取得できた後に、デコードを開始して、画像および音声データを出力するようにしている。したがって、図２１に示すような状況においても、一旦出力された画像および音声データが途切れるおそれがない。

【０１３４】次に、図２２に示すように、時点X1においてチャネル切換等があった場合について説明する。この場合には、時点X1においてＥＣＭデータを取得し、時点X2において復元した鍵Even1を得る。その後、ステップＳ１５、Ｓ２０を経て、ステップＳ１８においてデコードを開始する。したがって、時点X2より、画像および音声データの出力が得られる。

【０１３５】上記のようにこの実施形態においては、図２０や図２１に示す場合を除いて、チャネルの切換等から画像・音声が得られるまでの立ち上がり時間を、鍵復元に要する時間と等しくすることができる。ただし、図２０や図２１の場合には、最悪、鍵復元に要する時間の２倍の時間を要することとなる。

【０１３６】図２０の場合においても、復元処理の速い受信装置については、チャネルの切換等から画像・音声が得られるまでの立ち上がり時間を、鍵復元に要する時間と等しくすることが可能である。

【０１３７】そのためには、図２０のカレント鍵Odd0が取得できた時点X2において、下記の２つの条件を満足するか否かを判断し、満足している場合には、時点X2において画像・音声のＰＩＤをデコーダ７０に設定して、デコードを開始するようにすればよい。

【０１３８】条件１：時点X2が重複期間４０内にあること。

【０１３９】条件２：Δt2＞Δtrを満たすこと。

【０１４０】ここで、Δt2は重複期間４０の終了Teから鍵の切り替わる時点Txまでの時間、Δtrはこの受信装置による復元時間（ＥＣＭデータからスクランブル鍵を復元するに必要な時間）である。

【０１４１】条件１、２をともに満足する場合には、時点X2からデコードを開始し、画像および音声データを出力しても、以後、途切れることなく画像および音声データを出力することができる。したがって、このような判断を行うことにより、チャネル切換から画像および音声出力までの立ち上がり時間を短くすることができる。

【０１４２】なお、上記のような処理を行うためには、受信装置側においてΔt2の大きさが知られていなければならない。通信システムとして、Δt2が予め固定されている場合は、その値を受信装置に予め設定しておけばよい。また、Δt2が固定されていない場合には、送信装置からΔt2の値を受信装置に送るようにすればよい。

【０１４３】②２つの鍵復元を同時に並行して行う場合
上記では、受信装置における鍵の復元処理が、１つのＥＣＭデータごとに行われる場合について説明した。しかし、受信装置における鍵の復元処理が、図１５Ｂに示すように並行して行われる場合には、図１７の処理に換えて、図２３、図２４に示すような処理を行えばよい。

【０１４４】まず、図２５の時点X1において、チャネル

の切換または電源投入があって、このチャネルに対する処理が開始された場合について説明する。

【０１４５】まず、ＣＰＵ７２は、所望のチャネルの画像、音声データのスクランブル鍵に対応するＥＣＭデータのパケット符号PIDを、トランスポートデコーダ７０に設定し（ステップＳ５１）、当該ＥＣＭデータを選択的に取り出してメモリ７４に記憶する。

【０１４６】さらに、ＣＰＵ７２は、取得したＥＣＭデータのtable_idおよびtable_id_extensionを読んで、必要としているＥＣＭデータであるか否かを判断する（ステップＳ５１）。なお、処理開始時には、必要とするＥＣＭデータのtable_id、table_id_extensionの指定は行わないので、パケット符号PIDによって指定したＥＣＭデータであれば、無条件で指定条件を満たしたものとみなされる。

【０１４７】したがって、図２５の時点X1において、スクランブル鍵Odd0のＥＣＭデータを取得し、ステップＳ５２に進む。ステップＳ５２、Ｓ５４では、取得したＥＣＭデータのtable_id_extensionを見て、受信したＥＣＭデータが" カレント（ネクストあり）" か" ネクスト" であるかを判断する。つまり、重複期間４０内における受信であるかどうかを判断する。ここでは、重複期間４０外の受信であるから、ステップＳ５８に進む。

【０１４８】ステップＳ５８においては、ＥＣＭデータをＩＣカード８０に送る。ＥＣＭデータを受け取ったＩＣカード８０は、このＥＣＭデータからスクランブル鍵Odd0を復元し、時点X2においてＣＰＵ７２に送り返す（図２４、ステップＳ５９）。

【０１４９】スクランブル鍵Odd0を受け取ったＣＰＵ７２は、スクランブル鍵Odd0をデ・スクランブラ６８に設定する（ステップＳ６０）。これにより、デ・スクランブラ６８は、画像および音声データのスクランブルを解除してトランスポートデコーダ７０に出力するようになる。次に、トランスポートデコーダ７０に、所望のチャネルの画像データ、音声データのパケット符号PIDが設定されているかどうかを判断する（ステップＳ６１）。ここでは、まだ設定していないので、ステップＳ６２に進み、所望のチャネルの画像データ、音声データのパケット符号PIDをトランスポートデコーダ７０に設定する。

【０１５０】これにより、トランスポートデコーダ７０は、所望のチャネルの画像データ、音声データを、ビデオデコーダ８２、オーディオデコーダ８４に出力し始める。すなわち、図２５の場合には、時点X1にてチャネル切換が行われてから、ＩＣカード８０による復元処理時間経過後の時点X2より、画像および音声がＴＶセット８８から出力される。

【０１５１】次に、ＣＰＵ７２は、ＥＣＭデータのtable_id_extensionが" カレント（ネクスト無し）" であったかどうかを判断する（ステップＳ６３）。ここでは、" カレント（ネクスト無し）" であるから、ステップＳ６４に進み、受信すべきＥＣＭデータの変更を行う。ここでは、今回取得したＥＣＭデータと異なったtable_id（つまり偶数鍵）を持ち、table_id_extensionが" ネクスト" であるＥＣＭデータを取得するよう設定する。

【０１５２】次に、ネクスト鍵Even1のＥＣＭデータを取得すると（ステップＳ５１、図２５の時点X3）、ステップＳ５２、Ｓ５４、Ｓ５５を経てステップＳ５８に進む。ステップＳ５８、Ｓ５９においては、ＩＣカード８０にＥＣＭデータを送信し、ネクスト鍵Even1を得る（時点Ｘ４）。ＣＰＵ７２は、これをデ・スクランブラ６８に設定する（ステップＳ６０）。このようにして、ネクスト鍵Even1によってスクランブルされた画像データ、音声データが送られてくる前に、ネクスト鍵Even1をデ・スクランブラ６８に設定するので、画像および音声データを途切れることなく出力することができる。

【０１５３】次に、ＣＰＵ７２は、トランスポートデコーダ７０によって画像データ、音声データのデコードが開始されているか否かを判断する（ステップＳ２０）。ここでは、すでにデコードが開始されているので、ステップＳ６３を経て、ステップＳ６５に進んで、取得するＥＣＭデータの設定を変更する。

【０１５４】ステップＳ６５においては、カレントのＥＣＭ（つまり時点Ｘ１にて受信したＥＣＭ）のTable_id（つまり奇数鍵）を持ち、" ネクスト" のTable_id_extensionを持つＥＣＭを受信するよう設定する。その後、ステップＳ５１に戻って処理を繰り返す。

【０１５５】以後は、順次上記の処理を繰り返して、ＴＶセット８８にＮＴＳＣ画像信号と音声信号を出力する。

【０１５６】なお、図２６に示すように、チャネル切換の時点X1が重複期間４０の開始時点に近接している場合には、ネクスト鍵Even1のＥＣＭデータが送られてきていても、ＩＣカード８０がカレント鍵Odd0の復元処理を行っている状態となる。したがって、ネクスト鍵Even1の復元処理は、カレント鍵Odd0の復元処理が終わってから（時点X2,X3参照）ということになり、ネクスト鍵Even1の取得が後ろにずれ込むこととなる。

【０１５７】しかしながら、図１９のΔt1は、最も遅い処理の受信装置における２重復元時間（２つのＥＣＭデータから連続して２つのスクランブル鍵を復元するに要する時間）を基準として設定されているので、スクランブル鍵が変わる時点Txよりも早くネクスト鍵Even1をデ・スクランブラ６８に設定することができる。つまり、画像および音声が途切れることなく出力される。したがって、図２６に示す場合も、図２５と同じように、時点X1にてチャネル切換が行われてから、ＩＣカード８０による復元処理時間経過後の時点X2より、画像および音声がＴＶセット８８から得ることができる。

【０１５８】次に、図２７に示すように、時点X1においてチャネルの切換または電源投入があって、このチャネルに対する処理が開始された場合の処理を説明する。時点X1は重複期間４０内にあるので、カレントの鍵Odd0のＥＣＭデータとネクストの鍵Even1のＥＣＭデータが送られてきている。

【０１５９】ＣＰＵ７２は、取得したＥＣＭデータのtable_id_extensionから、そのＥＣＭデータによる鍵が、カレント鍵（ネクストあり）か、ネクスト鍵かを判断することができる（図８参照）。先に、時点X1においてカレント鍵Odd0のＥＣＭデータを取得した場合には、ステップＳ５２、Ｓ５３を経て、ステップＳ５６において、異なるTable_id（つまりEven鍵）を持つＥＣＭデータを受信するように設定する。このようにして、２つのＥＣＭデータを受信した後、これらをＩＣカードに送信する（ステップＳ５８）。この実施形態では、ＩＣカード８０は、２つの鍵の復元処理を同時に行うことができるので、ＣＰＵ７２は同時に２つの鍵を受け取る（時点Ｘ２）。したがって、時点Ｘ２から画像・音声の出力が得られる。

【０１６０】なお、ＣＰＵ７２からＩＣカード８０へのＥＣＭデータの伝送（伝送のための前処理や後処理を含む）、復元した鍵の伝送（伝送のための前処理や後処理を含む）には時間を要する。したがって、この実施形態のように同時処理を行うことのできるＩＣカードを用いることにより、ＣＰＵ７２がＥＣＭデータを受け取ってから、復元した鍵を得るまでの立ち上がり時間を短くすることができる。つまり、チャネル切換時等に映像・音声を得るまでの時間を短くすることができる。

【０１６１】次に、図２８に示すように、時点X1においてチャネル切換等があった場合について説明する。この場合には、時点X1においてＥＣＭデータを取得し、ステップＳ５２、Ｓ５４、Ｓ５８を経て、時点X2において復元した鍵Even1を得る。その後、ステップＳ６２においてＥＳのＰＩＤを設定し、デコードを開始する。したがって、時点X2より、画像および音声データの出力が得られる。

【０１６２】なお、この実施形態では、図２６に示すような場合において、Odd0の鍵が復元されるのを待って、Even1の鍵の復元処理を行っている。しかし、重複期間４０の開始時点Tsより、Even1の鍵の復元処理を並行して行うようにしてもよい。２つの鍵の復元を同時に行った方が、それぞれ単独で処理するよりも速いようなＩＣカード８０を用いる場合には、並行処理を行うことにより、重複期間４０を短くすることができる。

【０１６３】３．衛星放送システムにおける第２の実施形態

図２９に、他の実施形態におけるＥＣＭデータの送出タイミングを示す。この実施形態では、重複期間４０において、２つのスクランブル鍵を１つのＥＣＭデータとして送出するようにしている。したがって、重複期間４０以外では１つのＥＣＭデータに１つのスクランブル鍵が含まれ、重複期間４０では１つのＥＣＭデータに２つのスクランブル鍵が含まれることとなる。

【０１６４】図３０に、この実施形態におけるＥＣＭデータの構造を示す。table_id_extensionには、図２３の①②③④を区別する情報が記述されている。table_id_extensionが①③を示している場合には１つのＥＣＭデータが含まれ、②④を示している場合には２つのＥＣＭデータが含まれる。なお、この実施形態では、table_idは常に同一であり、奇数鍵、偶数鍵の区別をしていない。table_id_extensionのほうに、この情報が含まれているからである。

【０１６５】図３１に、重複期間４０近傍の拡大図を示す。重複期間４０の開始時Tsは下式のように定めるのが好ましい。

【０１６６】$Ts = Tx - Rmax - \alpha$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rmaxは、最大復元時間であり、想定される受信装置において１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間と、１つのＥＣＭデータから２つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も大きい合計復元時間をいう。αは余裕時間であり、０と等しいかそれ以上の値を持つ。

【０１６７】上記のように最大復元時間Rmaxを定めたのは、図３５に示すように、重複期間４０の直前の時点X1においてチャネル切換等があった場合を考慮したものである。この場合、復元によって鍵Odd0が得られた時点X2にて画像および音声データの出力を開始しても、スクランブル鍵が変わる時点Txより前に、ネクスト鍵Even1を取得することが保証される。これは、$\Delta t1$を、最も復元処理の遅い受信装置における合計復元時間以上に設定しているからである。

【０１６８】また、重複期間４０の終了時Teは下式のように定めるのが好ましい。

【０１６９】$Te = Tx - Rmin + \beta$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rminは最小復元時間であり、想定される受信装置において１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間と、１つのＥＣＭデータから２つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も小さい合計復元時間をいう。βは余裕時間であり、０と等しいかそれ以上の値を持つ。

【０１７０】この実施形態において用いる受信装置のブロック図は図１２に示すものと同じである。さらに、メモリ７４に記憶された受信処理プログラムのフローチャ

ートも、図１６に示す概略は同様である。しかし、図１６のステップＳ６のＥＣＭ、ＥＳの受信に関する処理の詳細が異なる。図３２に、この実施形態によるＥＣＭ、ＥＳの受信処理プログラムをフローチャートにて示す。

【０１７１】図３３に、この実施形態において用いる鍵再生装置１０２の全体構成を示す。この鍵再生装置１０２は、個数検出手段１０４と鍵再生手段１０６を備えている。個数検出手段１０２は、与えられた鍵対応データ中に何個の鍵が含まれているかを検出する。鍵再生手段１０６は、個数検出手段によって検出された個数の鍵を、鍵対応データから復元する。

【０１７２】この鍵再生装置１０２を、ＣＰＵを用いてＩＣカードとして実現した場合のハードウエア構成は、図１４に示すものと同じである。図３４に、ＩＣカード８０のメモリ９８に記録された処理プログラムのフローチャートを示す。

【０１７３】以下、図３２、図３４を参照して、この実施形態による受信装置９０の動作を説明する。

【０１７４】まず、ＣＰＵ７２は、所望のチャネルの画像、音声データのスクランブル鍵に対応するＥＣＭデータのパケット符号PIDを、トランスポートデコーダ７０に設定する（ステップＳ３１）。これにより、トランスポートデコーダ７０は、設定されたPIDを持つＥＣＭデータ（つまり所望のチャネルの画像、音声データのスクランブル鍵のＥＣＭデータ）を選択的に取り出してメモリ７４に記憶する。

【０１７５】さらに、ＣＰＵ７２は、取得したＥＣＭデータのtable_id_extensionを読んで、指定されたtable_id_extensionであるか否かを判断する。指定したtable_id_extensionを持ったＥＣＭデータでない場合には、受信を繰り返す。指定したtable_id_extensionを持ったＥＣＭデータであれば、ステップＳ３２に進む。ただし、チャネル切換時や電源投入時等の当該チャネルに対する処理開始時には、table_id_extensionを指定しないので、設定されたPIDを持つＥＣＭデータを受信すれば、ステップＳ３２に進むこととなる。

【０１７６】ステップＳ３２において、ＣＰＵ７２は、ＥＣＭデータをＩＣカード８０に送信する。ＩＣカード８０は、図３４のフロチャートに示すように、与えられたＥＣＭデータに２つの鍵が含まれているか否かを判断する（ステップＳ４１）。この判断は、ＣＰＵ７２から送られてくるtable_id_extensionや全体のデータ長等によって判断することができる。

【０１７７】２つの鍵が含まれている場合には２つの鍵を復元して送り返し（ステップＳ４２）、１つの鍵が含まれている場合には１つの鍵を復元して送り返す（ステップＳ４３）。なお、２つの鍵を送り返す場合には、何れが偶数鍵であり、何れが奇数鍵であるかを明らかにして送り返す。

【０１７８】図３４に戻って、ステップＳ３３においてスクランブル鍵を受け取ったＣＰＵ７２は、それがカレントの鍵であるかどうかを判断する。この判断は、当該鍵のＥＣＭデータ中のtable_id_extensionによって行うことができる。また、２つの鍵が含まれている場合には、先に現れるＥＣＭデータ（図３０のECM1）がカレント鍵であると定める等の方法により、いずれがカレント鍵かネクスト鍵かが分かるようにしている。

【０１７９】table_id_extensionには、図２９の①②③④を区別するための情報が記述されている。これにより、①②においてはカレント鍵が偶数鍵、③④においてはカレント鍵が奇数鍵であることを知ることができる。したがって、ＣＰＵ７２は、このtable_id_extensionに基づいて、受け取った鍵がカレント鍵であるか否か、あるいは、２つの鍵を受け取った場合には何れがカレント鍵であるかを知ることができる。

【０１８０】ＣＰＵ７２は、カレント鍵を受け取った場合には、これをデ・スクランブラ６８のＤＳデコーダに設定する（図１３参照）。これにより、デ・スクランブラ６８は、画像および音声データのスクランブルを解除して、トランスポートデコーダ７０に与える。

【０１８１】次に、ＣＰＵ７２は、table_id_extensionに基づいて、ネクスト鍵が送られてきているか否か、つまり②④であるかどうかを判断する（ステップＳ３５）。ネクスト鍵が送られてきていなければ、つまり①③であれば、重複期間４０内ではないので、ステップＳ３７を経て、トランスポートデコーダ７０に、所望のチャネルの画像データ、音声データのパケット符号PIDを設定する（ステップＳ３８）。これにより、トランスポートデコーダ７０は、所望のチャネルの画像データ、音声データを、ビデオデコーダ８２、オーディオデコーダ８４に出力し始める。

【０１８２】次に、ＣＰＵ７２は、取得すべきＥＣＭデータのtable_id_extensionを指定した後、ステップＳ３１に戻る。現在取得したＥＣＭデータのtable_id_extensionが①または④であれば、②または③を取得するよう指定する。現在取得したＥＣＭデータのtable_id_extensionが②または③であれば、①または④を取得するよう指定する。この指定によって、ステップＳ３１において、一度取得して必要のないＥＣＭデータを受信した場合には、ステップＳ３２以下に進まないようにしている。

【０１８３】以上のように、重複期間４０内にチャネル切換等によって処理を開始し、ＥＣＭデータを受け取った場合には、カレント鍵とネクスト鍵をデ・スクランブラに設定した後、デコードを開始するようにしている。また、重複期間４０外で処理を開始し、ＥＣＭデータを受け取った場合には、カレント鍵をデ・スクランブラに設定した後、デコードを開始するようにしている。なお、重複期間４０の終了時点Teから鍵が変わる時点Tx間での間は、ネクスト鍵が送られているが、table_id_ext

ensionではカレント鍵を送っているものとし、図３２における処理もこのtable_id_extensionに従うようにしている。

【０１８４】なお、この実施形態において、Δt1は、想定される最も復元処理の遅い受信装置において１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間と、１つのＥＣＭデータから２つのスクランブル鍵を復元するために要する復元時間との合計復元時間である最大復元時間Rmaxと等しいかまたはそれ以上に設定されている。したがって、図３５に示すように、重複期間４０の直前にチャネル切換等があった場合、いずれの受信装置においても、鍵が変わる時点Txより前にネクスト鍵を取得することができる。したがって、カレント鍵Odd0を取得した時点X2において画像および音声データを出力しても、途切れることなく画像および音声データを出力することができる。

【０１８５】一般的に、２つのＥＣＭデータを受けて２つの鍵を復元する時間よりも、２つの鍵が含まれた１つのＥＣＭデータから２つの鍵を復元する時間の方が短い。これは、前者の場合には、ＥＣＭデータをＩＣカードに送る処理、および復元された鍵を受信装置３０のＣＰＵ７２に送り返す処理を２回行わねばならず、その時間を要するからである。したがって、図２０に示すように、重複期間４０内においてチャネル切換等があった場合には、図１６、図１７に示す実施形態よりも、本実施形態の方が立ち上がり時間が短くなる。

【０１８６】なお、上記実施形態では、図２９の③にてカレント鍵Odd0を復元して取得した後、④にてカレント鍵Odd0とネクスト鍵Even1の双方を復元して取得するようにしている。したがって、すでに、取得済みのカレント鍵Odd0の復元を行っており、その分だけ復元時間が長くなっていた。これを解決するため、図３６に示すように、カレント鍵が取得済みである場合には、２つの鍵が含まれたＥＣＭデータを取得した場合であっても、ＩＣカード８０にてネクスト鍵だけを復元するように指示してもよい（ステップＳ３１Ｃ）。これにより、鍵の復元時間を短くすることができる。

【０１８７】以上のような処理を行うことにより、図３５に示すような場合に、時点X3にてＥＣＭデータを取得してから、復元が完了する時点X4までの時間が短縮される。したがって、重複期間４０の開始時点Tsを下式のように決定することができる。

【０１８８】$Ts = Tx - Rmax - \alpha$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rmaxは、最大復元時間であり、想定される受信装置において１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間と、２つのスクランブル鍵を含む１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も大きい合計復元時間をいう。αは余裕時間であり、０と等しいかそれ以上の値を持つ。

【０１８９】上記のように、Rmaxを図３２の実施形態に比べて小さくすることができるので、重複期間４０の開始時期を後ろにずらすことができる。これにより、重複期間４０を小さくして、ＥＣＭデータの送信密度を減らすことができる。

【０１９０】また、重複期間４０の終了時点Teを下式のように決定することができる。

【０１９１】$Te = Tx - Rmin + \beta$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rminは、最小復元時間であり、想定される受信装置において１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間と、２つのスクランブル鍵を含む１つのＥＣＭデータから１つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も小さい合計復元時間をいう。βは余裕時間であり、０と等しいかそれ以上の値を持つ。

【０１９２】上記のように、Rminを前記の実施形態に比べて小さくすることができるので、重複期間４０の終了時期を鍵の変わる時点Txに近づけることができる。これにより、処理の迅速な受信装置において、重複期間４０終了直前でチャネル切換があった場合の立ち上がり時間を短くすることができる。

【０１９３】なお、Teが後ろにずれることにより重複期間４０が長くなるが、これは、Tsが後ろにずれる量よりも小さいので、全体として重複期間４０は短くなる。

【０１９４】４．他のシステムにおける実施形態

上記実施形態では、衛星放送システムに適用した場合について説明した。しかしながら、暗号鍵を用いて行う地上波放送や有線放送についても同じように適用することができる。

【０１９５】また、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）等において、データを暗号化して通信する場合にも適用することができる。送信側と受信側が１対１の場合にも適用できるが、送信側から複数の受信側に一斉通信する場合に適用するとより好ましい。

【図面の簡単な説明】

【図１】この発明の一実施形態による通信システムの全体構成を示す図である。

【図２】この発明の一実施形態による通信システムにおける暗号化データと鍵対応データの送出タイミングを示す図である。

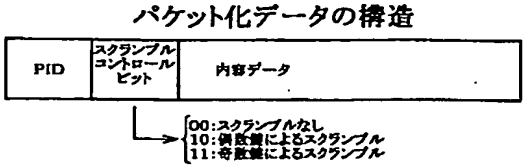
【図３】本発明を衛星放送システムに適用した一実施形態による送信装置の構成を示す図である。

【図４】送信装置によるデータのパケット化を示すための図である。

【図５】パケット化されたデータの構造を示す図である。
【図６】制御データＰＡＴの一例を示す図である。
【図７】制御データＰＭＴの一例を示す図である。
【図８】ＥＣＭデータの構造を示す図である。
【図９】制御データＮＩＴの一例を示す図である。
【図１０】ＥＳデータとＥＣＭデータの送出タイミングを示す図である。
【図１１】図１０の重複期間４０近傍の詳細を示す図である。
【図１２】本発明を衛星放送システムに適用した一実施形態による受信装置の構成を示す図である。
【図１３】デ・スクランブラ６８のＤＳレジスタの記憶内容例を示す図である。
【図１４】ＩＣカード８０の構成を示す図である。
【図１５】ＩＣカード８０における鍵復元処理のタイミングを示す図である。
【図１６】受信装置のメモリ７４に記録された受信処理のためのプログラムを示すフローチャートである。
【図１７】図１６のステップＳ６の処理の詳細を示すフローチャートである。
【図１８】チャネル切換が行われた場合の処理を説明するための図である。
【図１９】重複期間４０の直前にてチャネル切換が行われた場合の処理を説明するための図である。
【図２０】重複期間４０内にてチャネル切換が行われた場合の処理を説明するための図である。
【図２１】重複期間４０内にてチャネル切換が行われた場合の処理を説明するための図である。
【図２２】重複期間４０終了後、鍵変更時点Ｔxまでの間に、チャネル切換が行われた場合の処理を説明するための図である。
【図２３】２つの鍵復元を並行して行う場合における、図１６のステップＳ６の処理の詳細を示すフローチャートである。
【図２４】２つの鍵復元を並行して行う場合における、図１６のステップＳ６の処理の詳細を示すフローチャートである。
【図２５】チャネル切換が行われた場合の処理を説明するための図である。
【図２６】重複期間４０の直前にてチャネル切換が行われた場合の処理を説明するための図である。
【図２７】重複期間４０内にてチャネル切換が行われた場合の処理を説明するための図である。
【図２８】重複期間４０終了後、鍵変更時点Ｔxまでの間に、チャネル切換が行われた場合の処理を説明するための図である。
【図２９】他の実施形態における、ＥＳデータとＥＣＭデータの送出タイミングを示す図である。
【図３０】他の実施形態における、ＥＣＭデータの構造を示す図である。
【図３１】図３０の重複期間近傍の詳細を示す図である。
【図３２】他の実施形態における、図１６のステップＳ６の処理の詳細を示すフローチャートである。
【図３３】他の実施形態における鍵再生装置（鍵取得手段）の全体構成を示す図である。
【図３４】ＩＣカードのメモリ９８に記録されたプログラムのフローチャートを示す図である。
【図３５】チャネル切換が行われた場合の処理を説明するための図である。
【図３６】この実施形態において、図１６のステップＳ６の詳細を示すフローチャートである。
【図３７】従来の受信機の構成を示す図である。
【図３８】従来の鍵の通信方法を示す図である。
【図３９】従来の鍵の通信方法を示す図である。
【図４０】従来の通信方法における問題点を示す図である。

【符号の説明】
２０・・・送信装置
２２・・・鍵出力手段
２４・・・暗号化手段
２６・・・鍵対応データ生成手段
２８・・・送出手段
３０・・・受信装置
３２・・・受取手段
３４・・・復号化手段
３６・・・鍵取得手段

【図5】



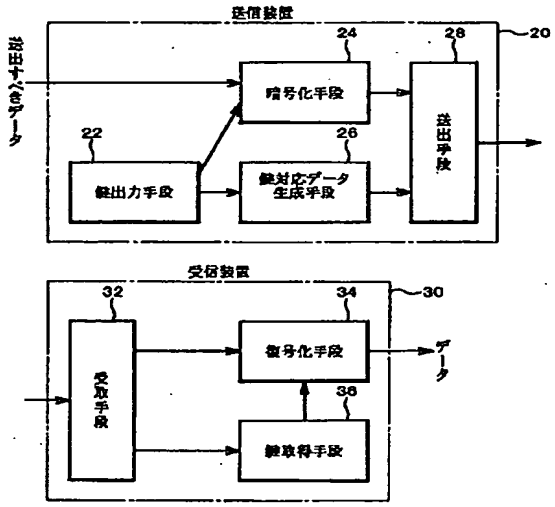
【図6】

PAT

チャンネルNO.	PMTのPID
3ch	◆×1◆
5ch	◆×11
7ch	◆×12

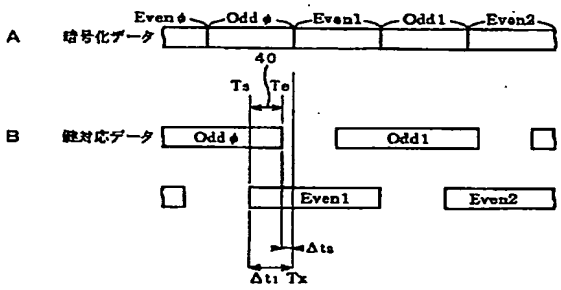
【図１】

システムの全体構成



【図２】

暗号化データと鍵対応データの送出タイミング



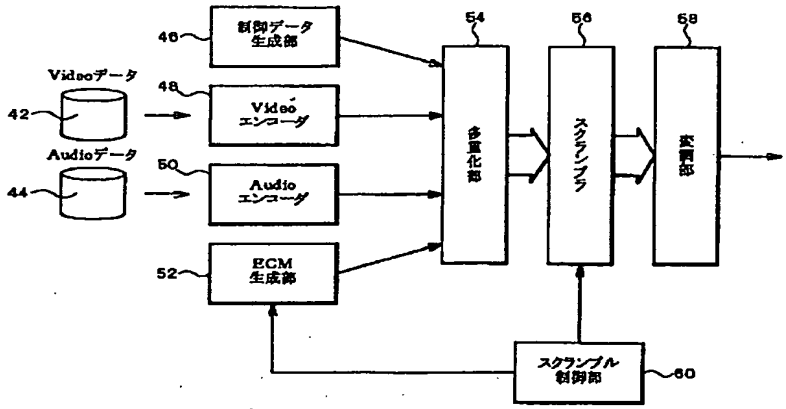
【図７】

PMT

ビデオ		オーディオ	
ECMのPID	ESのPID	ECMのPID	ESのPID
φ×21	φ×22	φ×21	φ×24

【図３】

送信装置の構成



【図１３】

デ・スクランブラのDSレジスタ

PID	Even鍵	Odd鍵
0×8T	101･･･1	110･･･1
0×75	――――	010･･･1

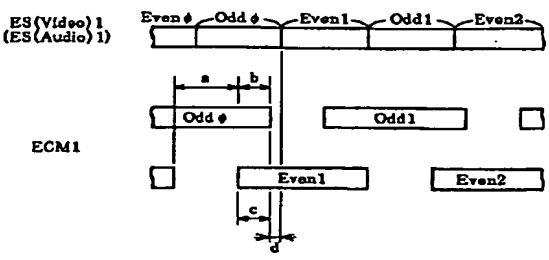
【図９】

NIT

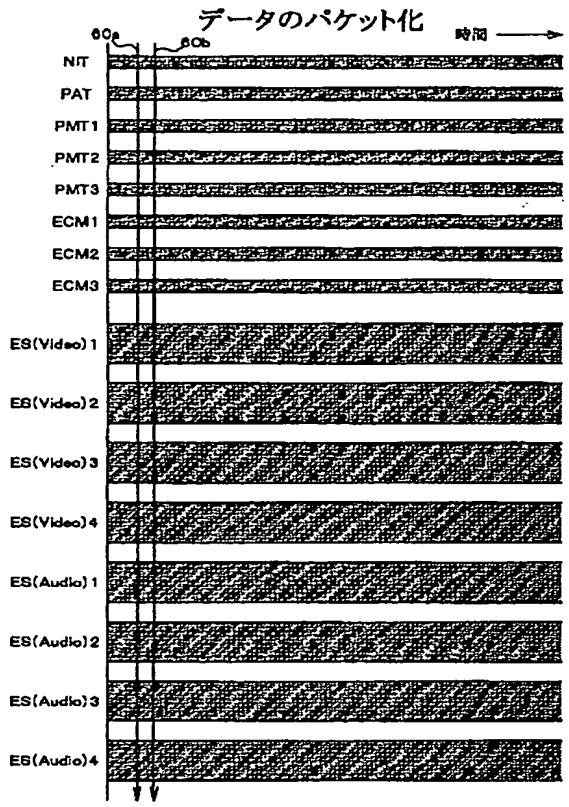
Ts_id	伝送経元	チャンネルリスト
0	11.2GHz、水平偏波･･･	0, 1, 2
1	11.23GHz、水平偏波･･･	3, 5, 7, 9
⋮	⋮	⋮

【図１０】

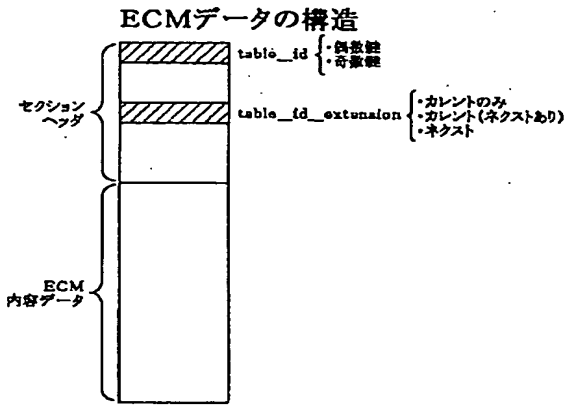
ESデータとECMデータの送出タイミング



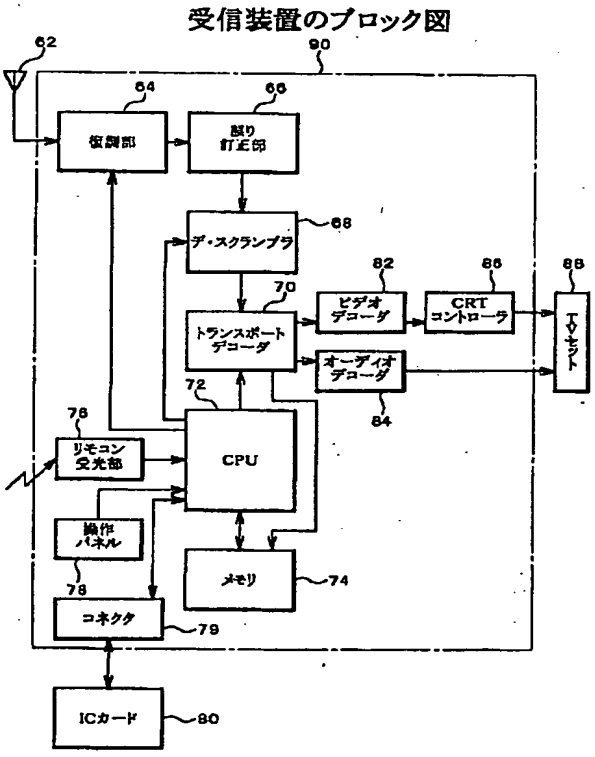
【図４】



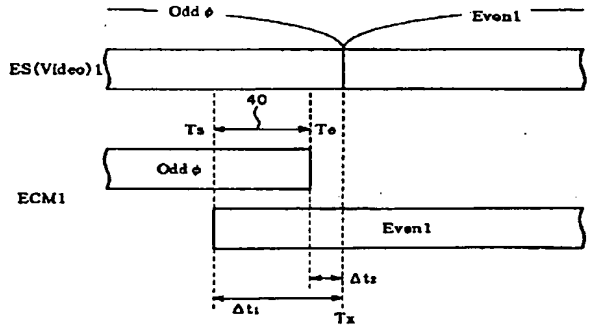
【図８】



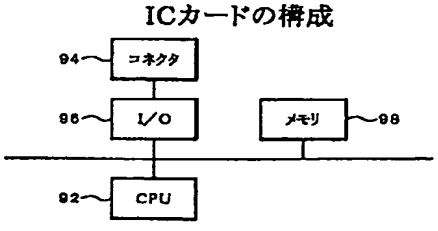
【図１２】



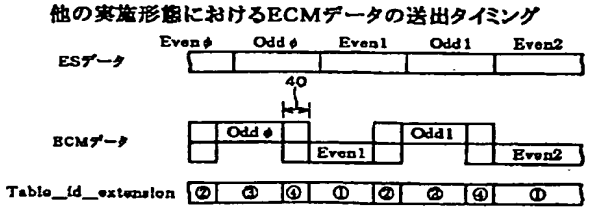
【図１１】



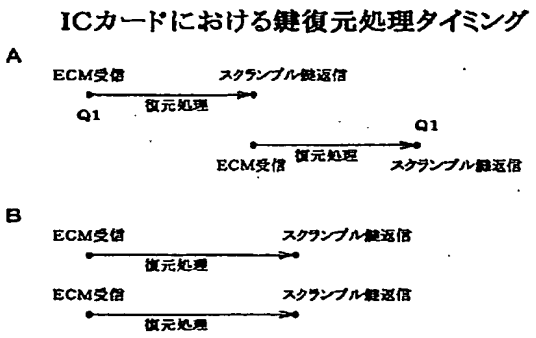
【図１４】



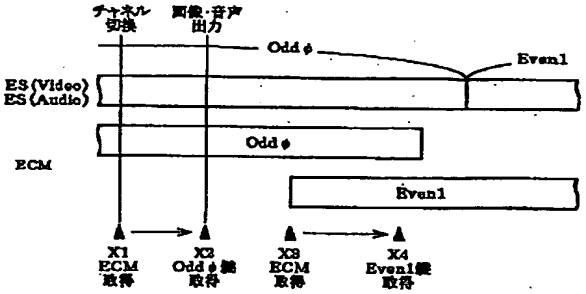
【図２９】



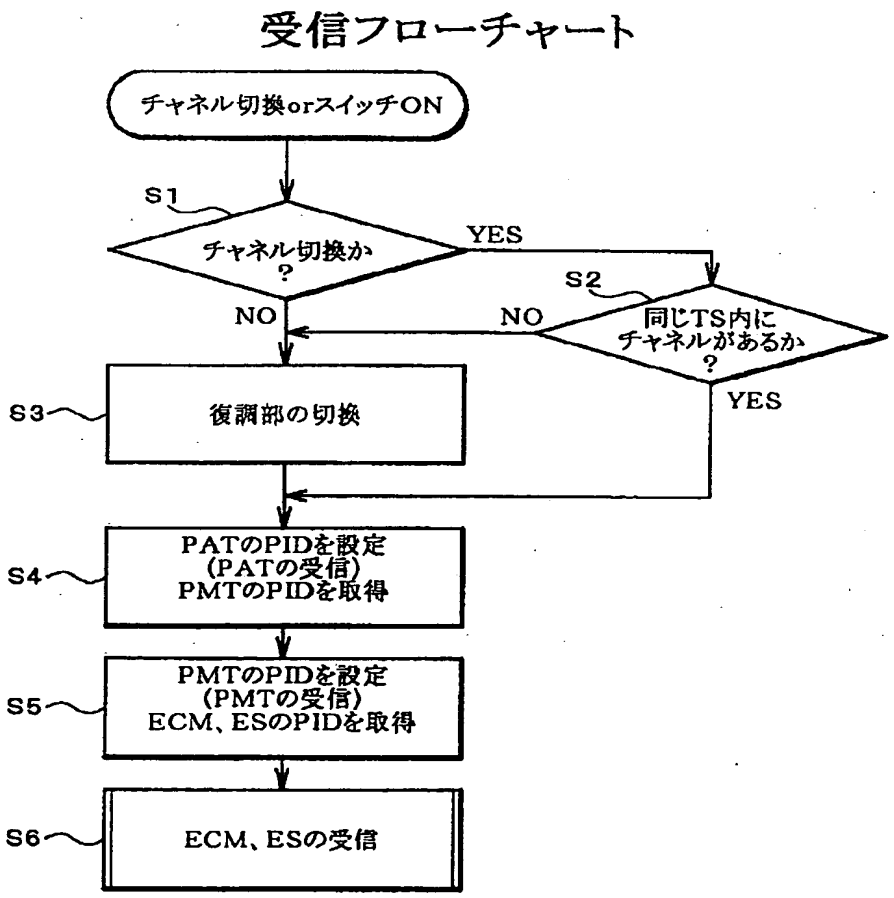
【図１５】


ICカードにおける鍵復元処理タイミング
A
ECM受信
スクランブル鍵返信
復元処理
Q1
Q1
ECM受信
復元処理
スクランブル鍵返信
B
ECM受信
スクランブル鍵返信
復元処理
ECM受信
スクランブル鍵返信
復元処理

【図１８】

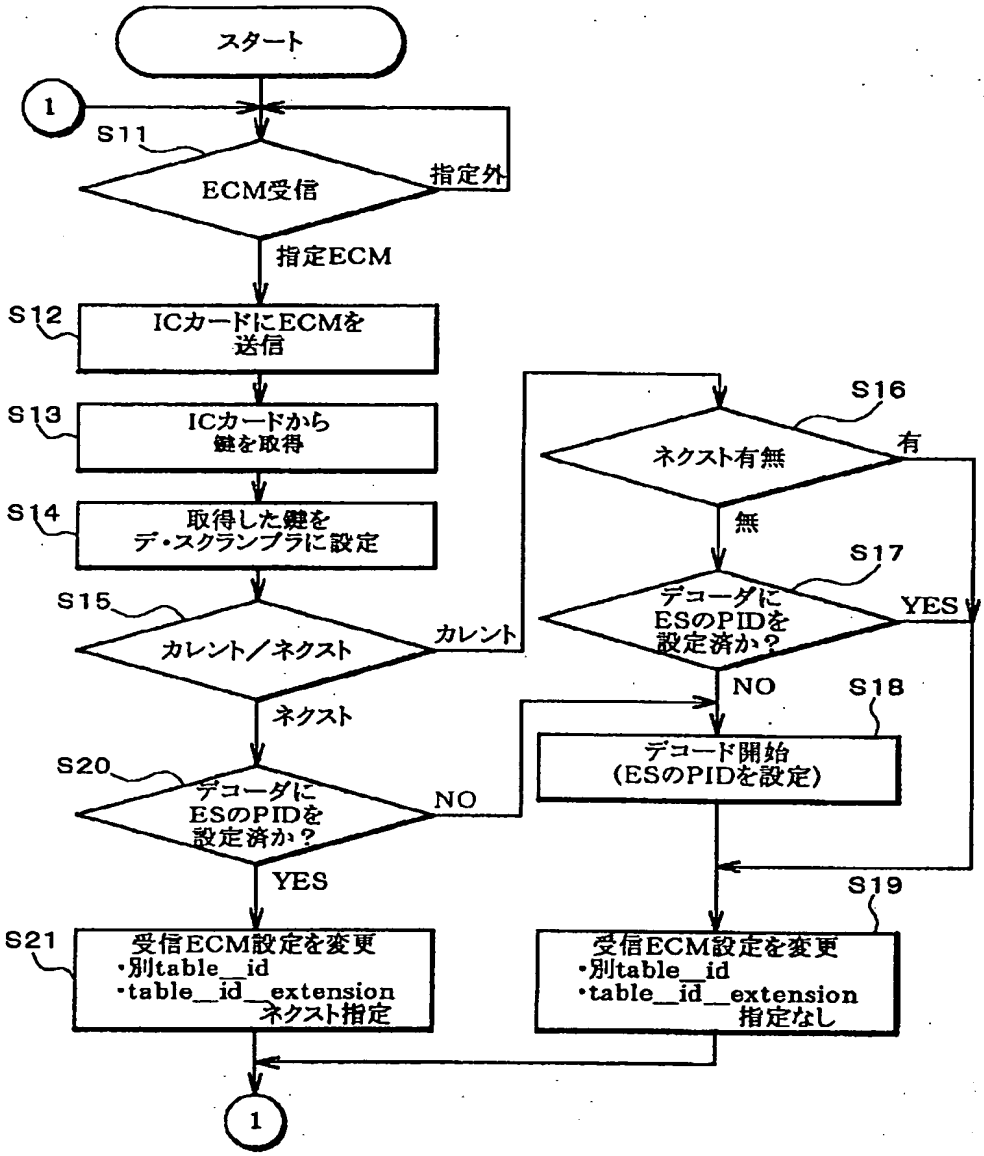

チャネル切換
画像・音声出力
Odd
Even1
ES(Video)
ES(Audio)
ECM
Odd
Even1
X1 ECM取得
X2 Odd鍵取得
X3 ECM取得
X4 Even1鍵取得

【図１６】

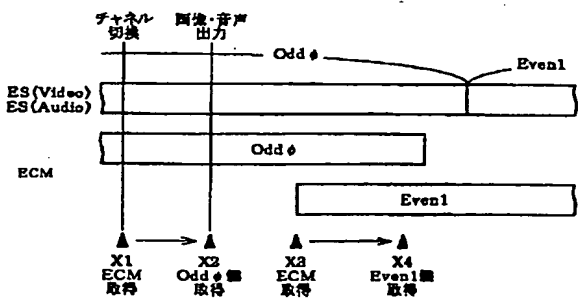

受信フローチャート
チャネル切換orスイッチON
S1
チャネル切換か？
YES
NO
S2
同じTS内にチャネルがあるか？
NO
YES
S3
復調部の切換
S4
PATのPIDを設定
(PATの受信)
PMTのPIDを取得
S5
PMTのPIDを設定
(PMTの受信)
ECM、ESのPIDを取得
S6
ECM、ESの受信

【図１７】

ECM、ESの受信処理(詳細) －鍵復元を1つずつ行う場合－

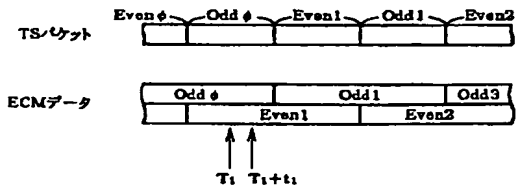


【図２５】

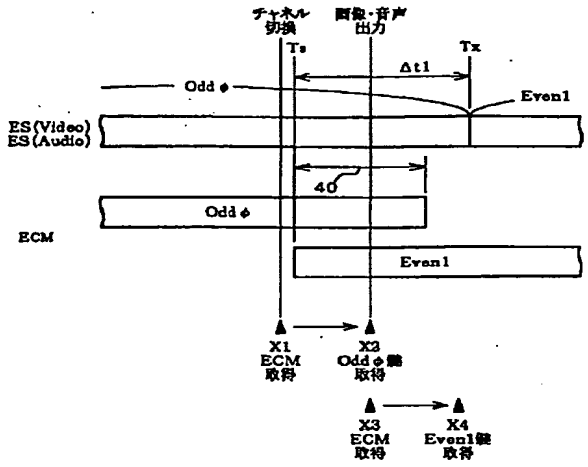


【図３８】

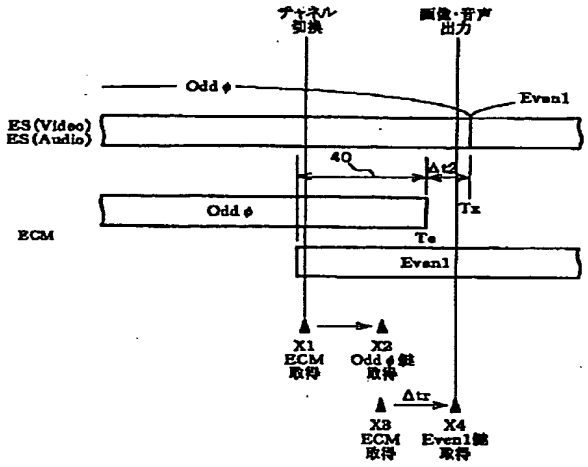
鍵の通信方法(従来技術)



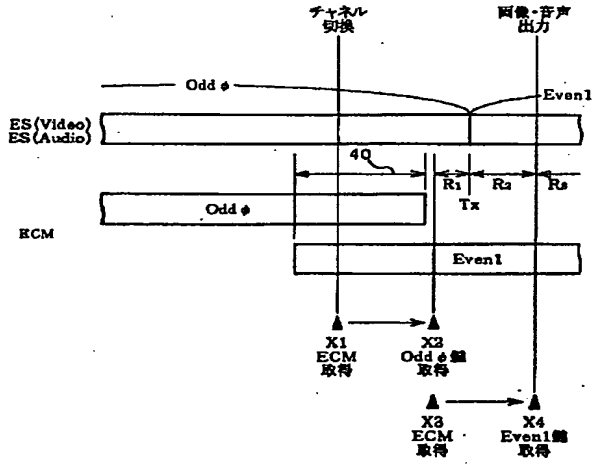
【図１９】



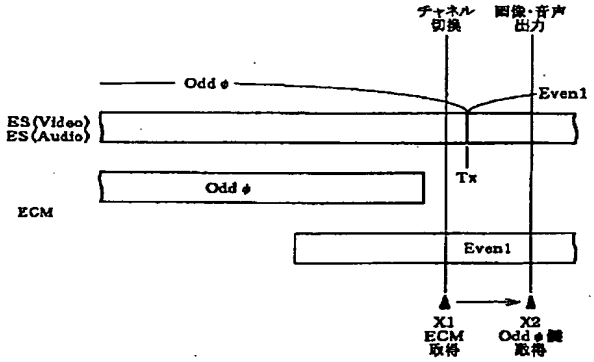
【図２０】



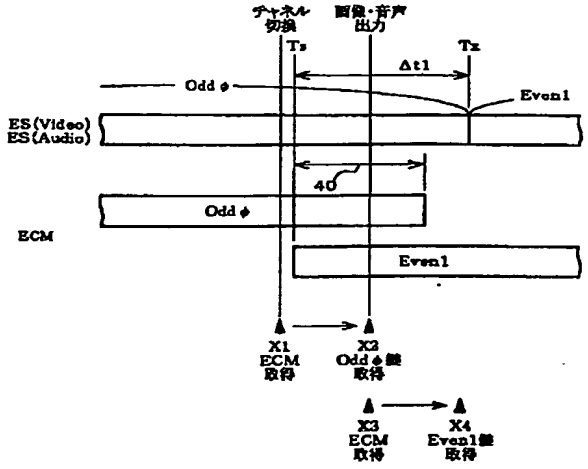
【図２１】



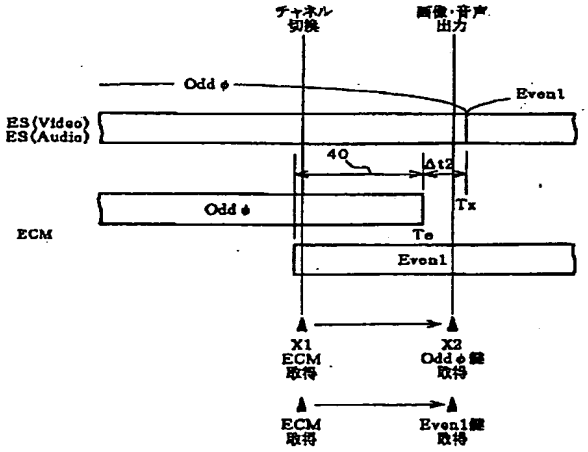
【図２２】



【図２６】

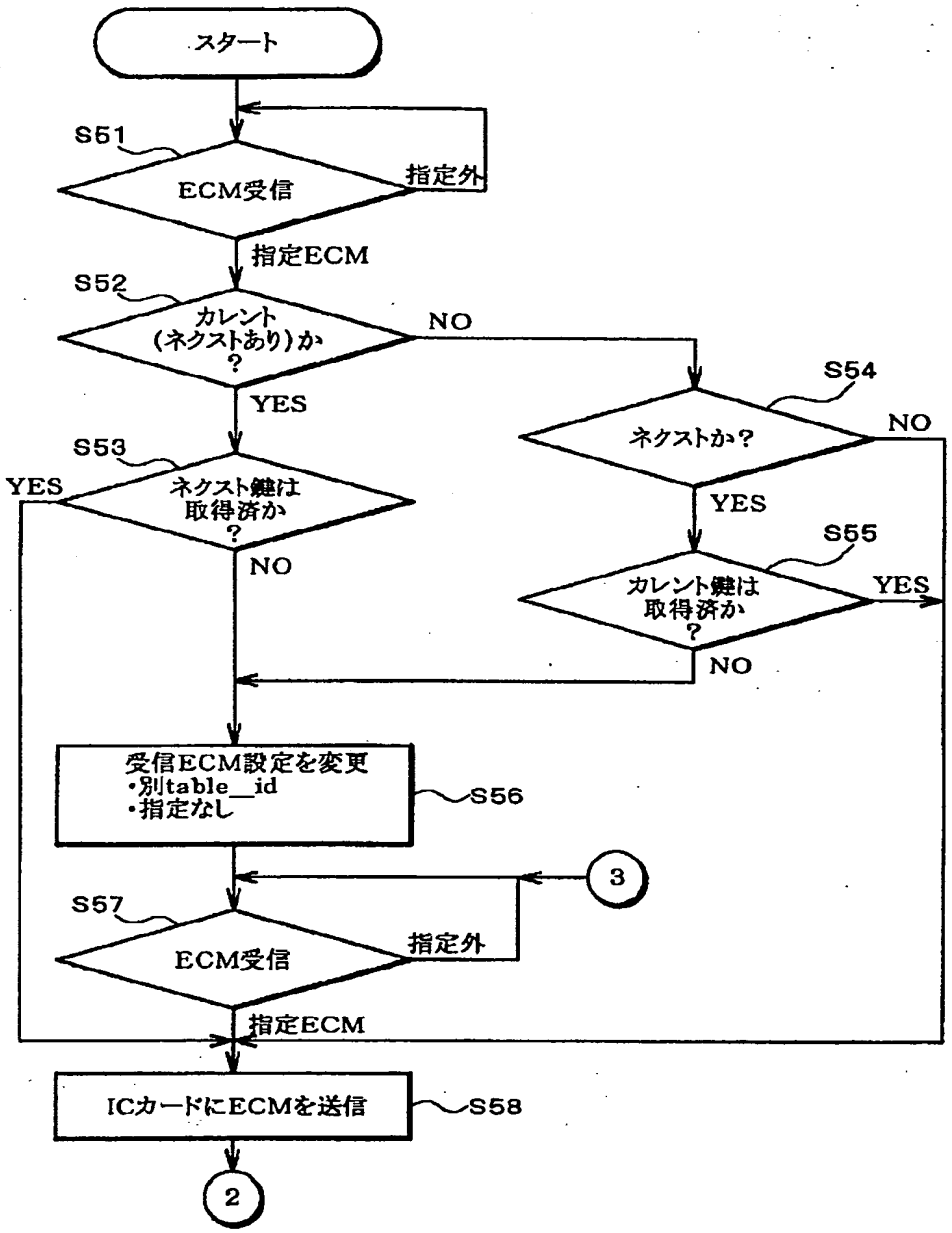


【図２７】



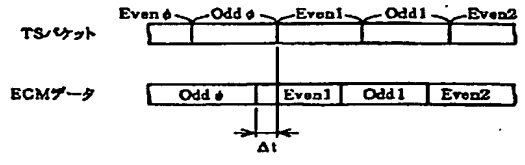
【図２３】

ECM、ESの受信処理(詳細)
－2つの鍵復元を同時に並行して行う場合－

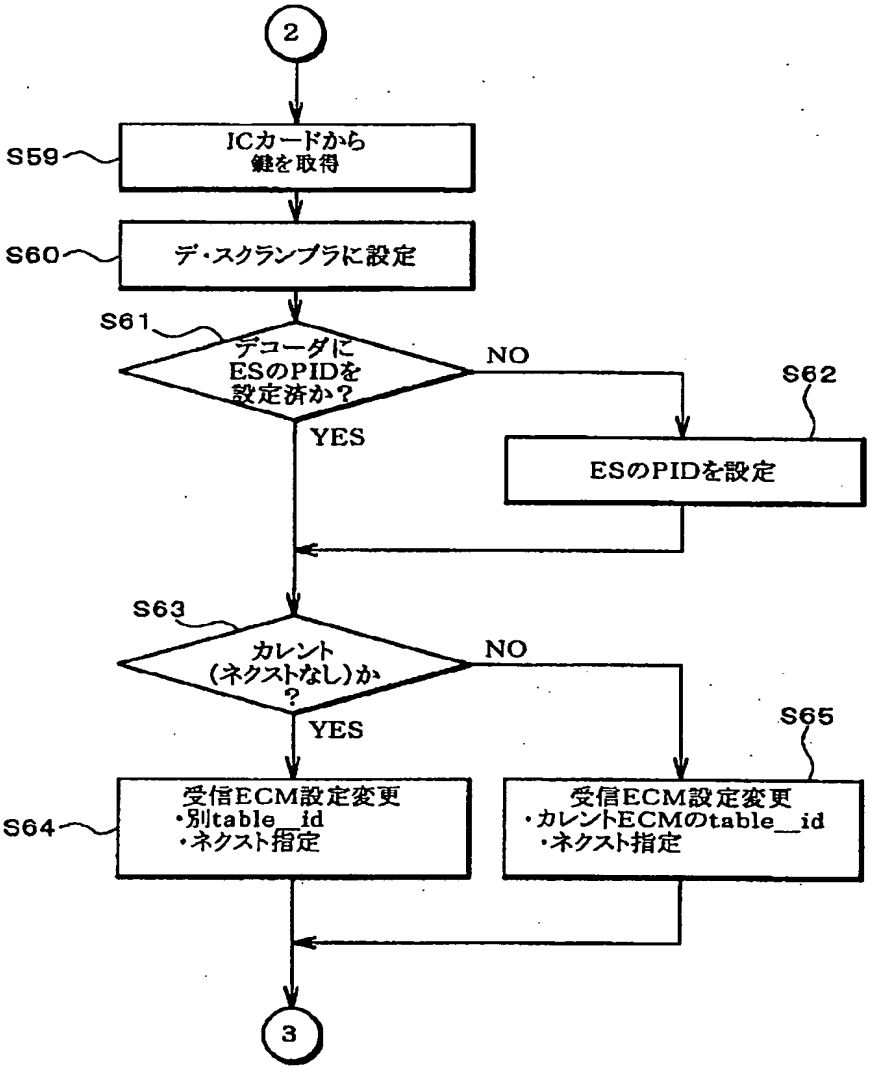


【図３９】

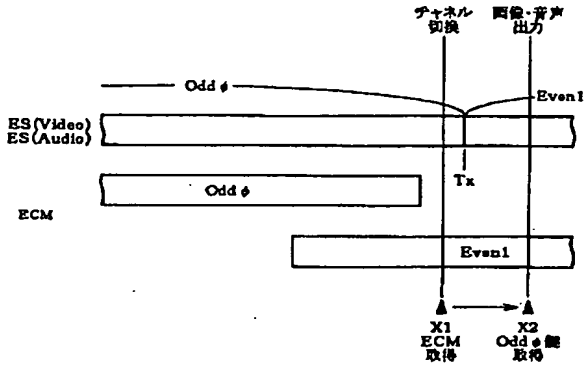
鍵の通信方法(従来技術)



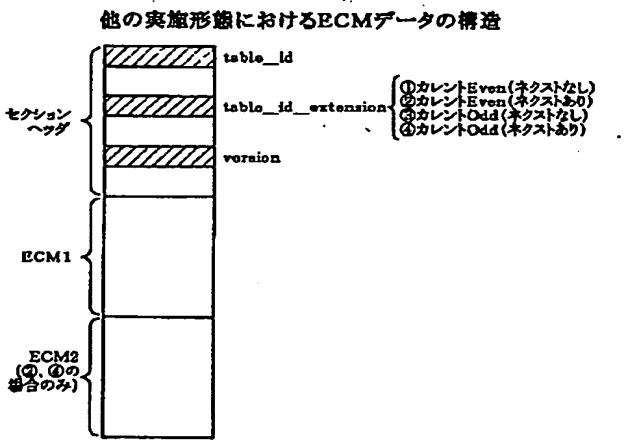
【図２４】


2
S59
ICカードから
鍵を取得
S60
デ・スクランブラに設定
S61
デコーダに
ESのPIDを
設定済か？
NO
YES
S62
ESのPIDを設定
S63
カレント
(ネクストなし)か
？
NO
YES
S65
S64
受信ECM設定変更
・別table_id
・ネクスト指定
受信ECM設定変更
・カレントECMのtable_id
・ネクスト指定
3

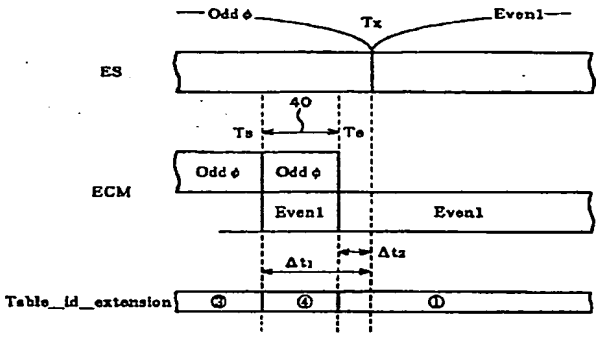
【図２８】


チャネル
切換
画像・音声
出力
Odd φ
Even1
ES(Video)
ES(Audio)
Tx
Odd φ
ECM
Even1
X1
ECM
取得
X2
Odd φ鍵
取得

【図３０】

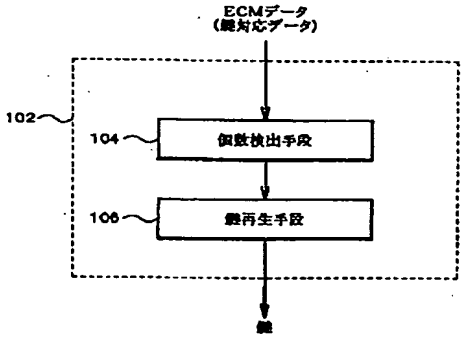

他の実施形態におけるECMデータの構造
table_id
table_id_extension
①カレントEven(ネクストなし)
②カレントEven(ネクストあり)
③カレントOdd(ネクストなし)
④カレントOdd(ネクストあり)
セクション
ヘッダ
version
ECM1
ECM2
(②、④の
場合のみ)

【図３１】



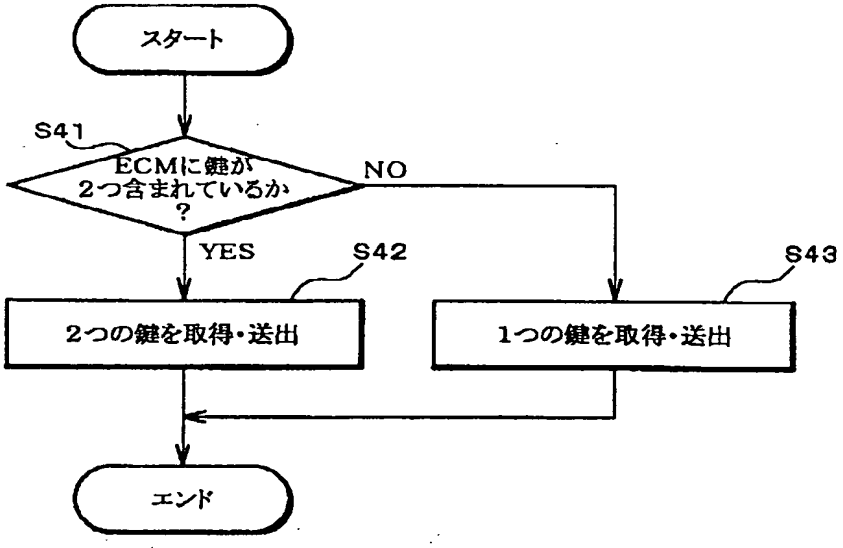
【図３３】

鍵再生装置（鍵取得手段）の全体構成

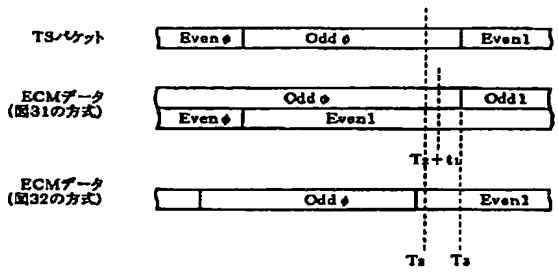


【図３４】

ICカードの処理フローチャート

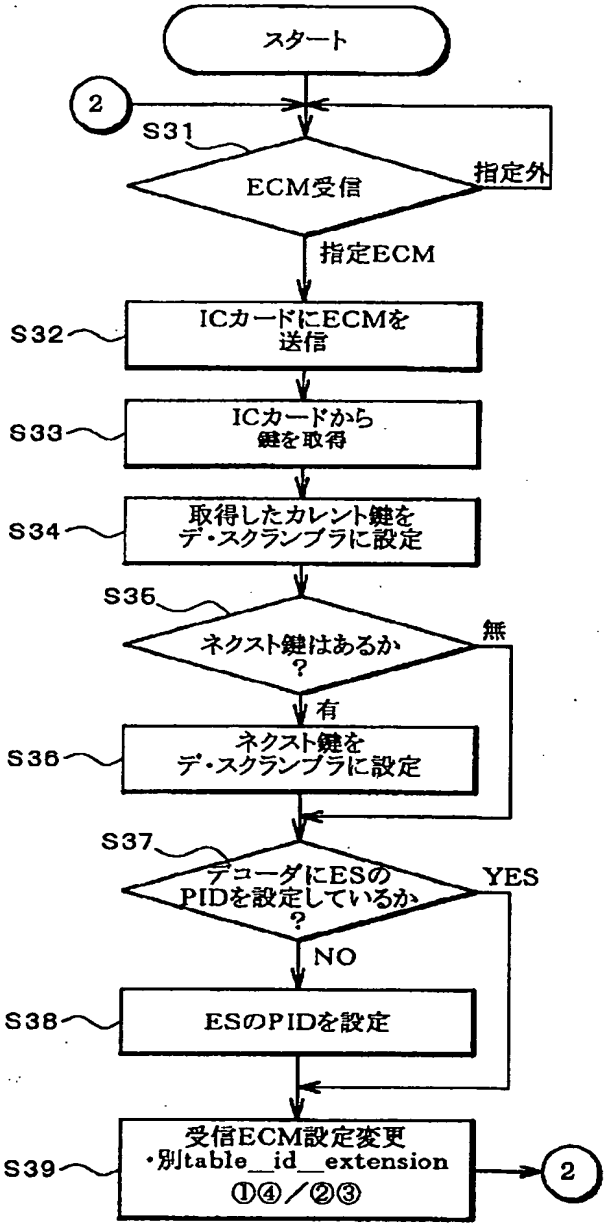


【図４０】

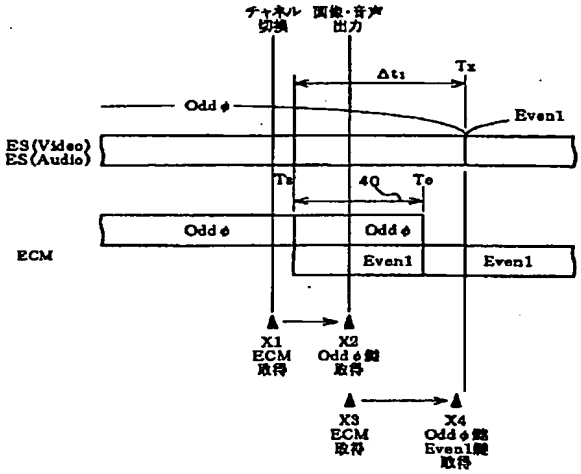


【図３２】

ECM、ESの受信処理(詳細)

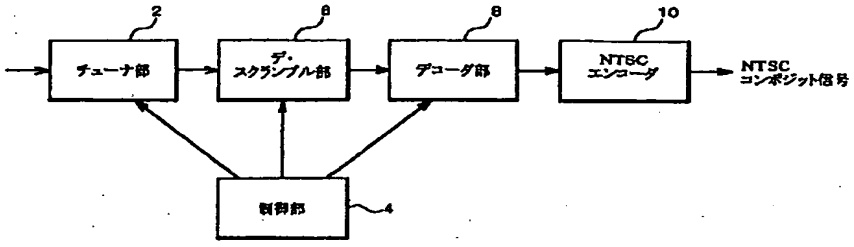


【図３５】



【図３７】

受信機の構成〈従来技術〉



【図３６】

ECM、ESの受信処理(詳細)